

世界数学名题欣赏丛书

科克曼女生问题

罗见今 著

辽宁教育出版社

1995年 • 沈阳

图书在版编目 (CIP) 数据

科克曼女生问题 / 罗见今著. — 沈阳: 辽宁教育出版社, 1995重印

(世界数学名题欣赏丛书)

ISBN 7-5382-1002-4

I . 科… II . 罗… III . 区组设计 IV . 0157.2

中国版本图书馆CIP数据核字(95)第16146号

科克曼女生问题

罗见今 著

辽宁教育出版社出版

辽宁省新华书店发行

(沈阳市北一马路108号)

沈阳市第二印刷厂印刷

字数: 127,000 开本: 787×1092 1/32 印张: 6 $\frac{3}{4}$ 插页: 4

印数: 3,001—7,000

1990年2月第1版

1995年12月第2次印刷

责任编辑: 俞晓群 谭 坚

责任校对: 杨力学

封面设计: 李国盛 李 飞

ISBN 7-5382-1002-4/G · 835

定 价: 7.30元

每函十三册, 总定价: 90.00元

内 容 简 介

本书是“世界数学名题欣赏丛书”之一。科克曼女生问题是1850年科克曼提出的，它的存在性成为组合数学区组设计的一大难题。女生问题与BIB、斯坦纳系、RBIB和科克曼系都有直接联系。本书引用较多资料，系统介绍这方面研究的历史和现状，特别是首次引用著名组合学家陆家羲在60年代初给出的科克曼女生问题的解，介绍了他的重大科研成果。本书从一个世界著名的数学游戏出发，阐述了区组设计的一些基本知识，把历史性、知识性和趣味性熔为一炉，可供大、中学生及广大数学爱好者阅读。

Summary

This book is one of "A Series of World Famous Mathematics-Appreciation". The Kirkman's schoolgirl problem was posed by T. P. Kirkman in 1850, its existence is one of the famous problems in block design of combinatorics. the schoolgirl problem is closely related to the BIB, Steiner systems, RBIB and Kirkman systems. This book systematically introduces the history of these problems and present condition, particularly quotes the solution of Kirkman's schoolgirl problem by the famous combinatorician Lu Jia-Xi in 1961—1965, and introduces his important results. It proceeds from the well-known game of Nim and expounds some elementary knowledge of block design. The historical taste, knowledge and interest are mixed together. It serves college students, middle school students and vast numbers of lovers of mathematics.

前言

组合数学是一门古老而又年轻的数学分支，它的起源可以追溯到人类初期计数的努力。中国是早期组合学思想的发祥地，我们的先人具有处理离散问题的高超本领。近三十年来，由于计算机科学的发展，促使这一古老的学科焕发了青春，绽开满树繁花，向世人展示了迷人的魅力。这里，我们撷取斯坦纳系的一簇，共同欣赏世界数学中的朵朵奇葩：科克曼女生问题、不相交斯坦纳三连系大集问题等的产生、发展和解决的历史进程。

科学史表明，科学对向她提供有价值思想的一切来源都表示出同样的尊重，无论是来自西方或东方，无论是来自贵族或平民、或衮衮诸公或

2 科克曼女生问题

莘莘学子，也无论是来自三教九流、卜筮占星、炼金炼丹、博奕娱乐……在本书里出现的中心人物斯坦纳、科克曼和陆家羲，他们虽有不同的文化和历史背景，但都出生于普通人家庭，没有受过大学数学的专门教育，靠着他们的勤奋，无师自通，自学成材，对科学作出了杰出的贡献。

“风起于青萍之末”，他们的成功之道，无不起于对数学强烈的兴趣和执著的追求。

组合设计的天才陆家羲是一颗过早陨落的新星。他曾走过了一条荆棘丛生的道路，他的名字载入了史册。人们对他二十五年不被理解的苦斗终会渐渐淡漠。是的，人类要为科学的胜利付出代价，为了新芽能破土而出，多少优秀的人们奉献了自己的生命。当陆老师逝世六周年之际，谨以这本小书寄托作者深切怀念之情。

作者从事科学史工作，从中学时就爱好数学，受到陆老师之死的震动而进入研究组合设计史的领域，想搞清楚问题的来龙去脉、难度、科学价值和历史地位。当写本书时，又踌躇再三，深有“如履薄冰、如临深渊”之感。幸而能借助于较多的资料，有的是陆老师遗文，有的通过卫星取自美国Dialog信息库，有的辗转取自国外学者未发表的文献目录。希望有心的读者参考所引文献，以免有偏颇之虞。

作者对苏州大学吴利生教授、河北师院康庆德教授曾给予的帮助，对陆家羲夫人张淑琴医生、中国科学院合肥计算中心顾同新副研究员所提供的研究资料表示感谢。

本书错漏不当之处在所难免，深望读者不吝指正。

罗 见 今

1989年于呼和浩特

目 录

前 言	1
一、从中国Nim游戏谈起	1
二、组合数学与区组设计简介	11
三、科克曼女生问题的提出	23
四、关联矩阵及其在区组设计中的应用	35
五、有限域和有限射影平面的应用	51
六、斯坦纳系和斯坦纳三连系	63
七、斯坦纳三连系和斯坦纳系的 构造方法	77
八、科克曼系和科克曼三连系	99
九、陆家羲：科克曼女生问题的解	111
十、斯坦纳系的相交性问题	131
十一、不相交斯坦纳三连系大集定理	143

2 科克曼女生问题

十二、关于Nim型对策和Nim三连系.....159

[附录]陆家羲：平衡不完全区组与

可分解平衡不完全区组的构

造方法177

参考文献192

译名对照202

Contents

Preface	1
1. On the Chinese game of Nim.....	1
2. Combinatorics and block design	11
3. The Kirkman's schoolgirl problem.....	23
4. Combinatorial matrix and its application	35
5. Finite field and finite projective plane	51
6. Steiner systems and Steiner triple systems	63
7. The methods of construction of $S(t, k, v)$	77

2. 科克曼女生问题

8. Kirkman systems and Kirkman triple systems.....	99
5. Lu Jia-Xi, the solution of Kirkman's schoolgirl problem.....	111
10. Intersection properties of Steiner systems.....	131
11. On the theorem of large sets of disjoint Steiner systems	143
12. The game of Nim and Nim triple systems	159
Appendix Lu Jia-Xi, The methods of constrution of BIB and RBIB (March, 14, 1965.)	177
References	192
A List of Chinese English Names	202

一、从中国Nim游戏谈起



在我国民间，流传着一种二人数学游戏。它的规则是：有 k ($k \geq 3$) 堆物件，两人轮流从中拿取，每次限于拿其中的一堆，至少取一个，至多取一堆；最后一个轮谁取谁负（或胜）。这种游戏，以 $k=3$ 时最基本、最有趣，北方流行的名称叫做“抓三堆”；南方粤语叫“拧法”，又名“翻摊”；国外称它为 Chinese game of Nim⁽¹⁾，或者 simple game of Nim⁽¹⁾，或者 Fan Tan⁽²⁾，或者就叫做 Nim⁽³⁾。Fan Tan 就是“翻摊”，Nim 就是“拧法”，都暗示了这种游戏源于中国。这样说，并不是望文生义，尽管迄今尚未从我国古文献中发现有关它的记载，然而有根据认为，Nim 是我国古代流传至今的游戏，现已遍及全世界，并引起了数学界的兴趣与重视。按照我国古代的传说，数学游戏一类的“奇技淫巧”，被认为是不足以登大雅之堂的；就连博弈，“今夫奕之为数，小数也”，不过是雕虫小技。因此，象“翻摊”一类的游戏，难以在经、

史、子、集中留下详细记录是可以理解的。然而，伴随着计算机科学的崛起，离散数学、组合数学和图论获得了迅猛的发展，当人们以一种全新的观点回过头去观察古代的游戏时，人们吃惊地发现那里边包含了许多现代数学深奥的道理。无怪乎美国数学家布鲁尔迪说：“组合数学发源于数学消遣和游戏。无论为了消遣还是由于它们的美学兴趣，过去所研究过的许多问题对于当代的纯粹科学或应用科学都是非常重要的。”^①从数学游戏开始居然能发展成一门深刻的现代数学分支，这是许多玩过数学游戏的人们始料不及的吧！本书就是企图用这样的观点，回过头来看看“抓三堆”的游戏。

假定上述规则确定为“最后一物谁取谁负”，那么，经过若干次试验，运用逻辑推理和数列的知识，可以发现一些规律。把三堆的数字记作 $\{x, y, z\}$ ，它们是不同为零的非负整数，显然， $\{0, 0, 1\}$ 和 $\{1, 1, 1\}$ 的局面谁取谁负；同样易知， $\{n, 0, n\}$ ($n > 1$) 的局面也是谁取谁负，当 $n = 2$ ，对手取 1，你取 2；对手取 2，你取 1；当 $n > 2$ ，对手不论取多少，只要不余下 1，你就取出和他相同的数目，最后必然出现 $\{2, 0, 2\}$ 的格局留给对手。

在三个数字中最小数为 1 时，创造 $\{1, 2n, 2n+1\}$ 的格局是制胜的， $\{1, 2n, 2n-1\}$ 的格局则导致失败。前者轮对手取时，他有如下的选

取法：取第1堆之1，你可取第3堆之1，造成 $\{n, 0, n\}$ ，对手必败；对手取第2堆，只要不留下0，1，你可从第3堆里仿照他取多少，你就取多少，这样仍保持 $\{1, 2n, 2n+1\}$ 格局不变；对手取第3堆时，你的对策类似上法。于是，我们可以得到制胜方案：

$\{0, 0, 1\}$			
$\{1, 1, 1\}$	$\{2, 0, 2\}$	$\{3, 0, 3\}$	$\{4, 0, 4\}$
$\{1, 2, 3\}$	$\{2, 1, 3\}$	$\{3, 1, 2\}$	$\{4, 1, 5\}$
$\{1, 4, 5\}$	$\{2, 4, 6\}$	$\{3, 4, 7\}$	$\{4, 2, 6\}$
$\{1, 6, 7\}$	$\{2, 5, 7\}$	$\{3, 5, 6\}$	$\{4, 3, 7\}$
$\{1, 8, 9\}$	$\{2, 8, 10\}$	$\{3, 8, 11\}$	$\{4, 8, 12\}$
$\{1, 10, 11\}$	$\{2, 9, 11\}$	$\{3, 9, 10\}$	$\{4, 9, 13\}$
$\{1, 12, 13\}$	$\{2, 12, 14\}$	$\{3, 12, 15\}$	$\{4, 10, 14\}$
$\{1, 14, 15\}$	$\{2, 13, 15\}$	$\{3, 13, 14\}$	$\{4, 11, 15\}$
.....
$\{5, 0, 5\}$	$\{6, 0, 6\}$	$\{7, 0, 7\}$	
$\{5, 1, 4\}$	$\{6, 1, 7\}$	$\{7, 1, 6\}$	
$\{5, 2, 7\}$	$\{6, 2, 4\}$	$\{7, 2, 5\}$	
$\{5, 3, 6\}$	$\{6, 3, 5\}$	$\{7, 3, 4\}$	
$\{5, 8, 13\}$	$\{6, 8, 14\}$	$\{7, 8, 15\}$	
$\{5, 9, 12\}$	$\{6, 9, 15\}$	$\{7, 9, 14\}$	
$\{5, 10, 15\}$	$\{6, 10, 12\}$	$\{7, 10, 13\}$	
$\{5, 11, 14\}$	$\{6, 11, 13\}$	$\{7, 11, 12\}$	
.....	

表1. “抓三堆”Nim制胜方案

6 科克曼女生问题

不难据此得出各列三堆数目的通项公式：

$$\begin{aligned} &\{1, 2n, 2n+1\}; \{2, 4n, 4n+2\}, \\ &\{2, 4n+1, 4n+3\}; \\ &\{3, 4n, 4n+3\}, \{3, 4n+1, 4n+2\}; \\ &\{4, 8n, 8n+4\}, \{4, 8n+1, 8n+5\}, \\ &\{4, 8n+2, 8n+6\}, \\ &\{4, 8n+3, 8n+7\}; \text{等等。} \end{aligned}$$

除 $\{0, 0, 1\}$ 和第一行之外，表1中横线以上的各组（我们称为三元组）都是重复出现的，依自然数顺序，不难找出各列三元组排列的“花样”，从而把这个数表向下方、向右方编排下去，因而全部方案，都是已知的了。

但是，这种结果除了较繁之外，它没有揭示游戏的数学本质，也没有回答为什么能够制胜的原因。当你没有掌握它的规律时，你不可能手拿一张数表同你的朋友去作这游戏。那样做不仅于对方不公平，而且显得你自己并不聪明。事实上，Nim发展的历史也告诉人们，正由于它的规则十分简单，但要掌握一种简便的制胜方法却不容易，这就激励人们在反复的试验中寻找它。

Nim具有悠久的历史，它是古代博奕思想遗留至今的样本。一位美国研究者认为，Nim是世界上最古老的游戏，它起源于几千年前的东方^[1]。最早传到西方的Nim用最简单的材料：十几块石子，通常摆成3、4、5三堆，或者3、5、7三堆。游戏规则同上所述，最后一件谁取谁负，

现在叫做LPL (Last player losing)型Nim。流传到西班牙的Nim，最后一件谁取谁胜，现在叫做LPW (Last player winning) 型Nim。在表1中第1列前两个数组换成 $\{1, 0, 1\}$ ，就是LPW型Nim的制胜方案，可知两者之间没有本质的区别。

也许有人会问：既然西方学者也认为Nim源于东方，源于中国，那么为什么称为Nim呢？除了上述Nim就是“拧法”的推测之外，有必要从语源学的角度追溯它的根源。Nim是一个英语古动词，不见于一般英文字典。《牛津英语词典》里说：nim “大多数应用同后来的动词‘拿，取’

(take, 源出斯堪的纳维亚语) 的各种含义相一致，15世纪之前一直通用，16世纪的文献中只留下了它很少的足迹，但在1600年后它突然间变成了一个俚语或俗语，意为小偷小摸 (to steal, filch, pilfer)。整个17世纪，这一用法非常流行。”⁵⁾ 在nim即take的意义上，Nim转化为一类数学游戏的名词。《韦氏新国际辞典》对Nim的解释说：“将算筹(counters)摆成一堆或若干堆，每堆的数目是商定的，游戏双方轮流从中抽取一根或若干根，目的在于取到最后一根筹，或迫使对手取到它，或以取到筹数的多少论胜负。”⁶⁾

语源学的根据似乎给我们以启迪：Nim作为数学游戏的名称，在西方不迟于15世纪，所用

的东西是算筹、筹签或筹码，它的玩法不止一种。不少人称它为“火柴游戏”，只是近代的叫法，说明近人取用火柴之便，尚不如称为“算筹游戏”考之有据。至于有人说福建、台湾一带闽语中“拿取”一词发音为nim，可能由此流传国外，我们却无法断定五百年或七、八百年前闽语中nim之音代表什么意思，也无法考证它是如何流传出去的，又是怎样变成了英语外来词的。还有资料记载⁽⁷⁾，Nim在19世纪末叶开始传入欧洲，这是不确切的。实际上19世纪末已经有组合数学家对Nim进行了研究，例如穆尔(E.H. Moore)提出了一种P阶Nim，成为图论Nim型对策第三定理的主要例子。⁽²⁾

几千年来，Nim给人们带来了娱乐。斗智决胜的心理，促使人们暗中摸索，寻找在各种情况下能揭示正确取法的一般原则。1901年，美籍法国数学家布顿(C.L. Bouton)成功的——他用一种精巧的分析方法，找到了一个非常简单的原则，任何人都能应用。用这个原则能使你知道哪是负局，哪是胜局，以及在后一种情况下如何取才能保证获得最后胜利。我们先来看现在破解Nim的方法，以抓三堆为例，任取三堆的数字为11, 22, 29，用二进制数表示出来：

$$(11)_{10} = (1011)_2$$

$$(22)_{10} = (10110)_2$$

$$(29)_{10} = (11101)_2$$

$$\underline{\hspace{1.5cm}} \\ 00000$$

上式所进行的运算是一种特殊的加法，即 $1+1=0$ ， $1+0=1$ ， $0+0=0$ 。只要照此办理加出来的和为0，那么不管下一位轮到谁来取，也不管他采用任何一种取法，等待他的必然是失败（当然前者须保证步步不错）。这样的加法在数学上叫“点加”或“模2加”，所得之和叫“点和”或“布尔和”，在研究群、环、域的近世代数或逻辑代数中很有用。如果点和不为0，那么轮谁取，谁便交了好运。正确的取法只有一个，取完后仍能保持三数点和为0，这一难堪的局面仍然甩给他对手——文末还要证明正确取法的唯一性。

这样，古代的游戏变成了一个漂亮的数学问题的解。但是作为一种游戏，却被破坏无遗，因为假定双方都掌握了破解原则，游戏胜负一望即知，就变得索然无味了。事情到此似乎已全部结束。然而，出人意料的是，世界上真有这样仗义的人，他路见不平，挺身而出，向布顿的研究结果提出挑战：他就是丹麦作家、科学家和发明家皮特·海因(Piet Hein)。他以复兴Nim为己任，力图归还Nim作为一个不可征服的游戏的古老尊严，他对Nim所作的改变将不减弱原则的简易性，并在布顿分析所及的范围之外。

Nim的确是数学游戏中的皇后，西方数学家开玩笑地把布顿的分析称作“行刺”事件。到本世纪50年代，皮特·海因大功告成，他完成了自己确定的这一离奇而困难的任务。最难的是保留游戏规则的简易性，同时应使布顿的分析方法对这个新的Nim失效。皮特·海因的新Nim由加德纳(M. Gardner)写成一篇文章在《科学的美国人》杂志上发表，并收入他的一本关于数学谜题与游戏的书中⁽²⁾。在二十年的时间里，数学家们企图破解新Nim，努力去找一个一般的原则，它将适用于具有可变数字的所有Nim变型，一如布顿对可敬的原Nim所作的分析那样。但是，他们的努力迄今为止都是徒劳的⁽³⁾。也许皮特·海因的研究是如此之彻底，它将永远保证Nim作为一种游戏的历史地位。

关于Nim的历史和解法的初步讨论到此先告一段落，作为本书的引子，在叙述完下两节之后，我们将会发现：表1抓三堆Nim制胜方案中，每列横线以下的三元组（共35个），恰恰是科克曼十五女生问题的一组解！

二、组合数学与区组 设计简介



科克曼女生问题是组合数学区组设计中的一个世界名题。在介绍女生问题之前，有必要对它产生的这一学科分支作一概略的介绍。

组合数学是离散数学(discrete mathematics)“大家庭”的主要成员之一。所谓数学是离散的，主要是说它的研究对象不是连续(continuous)的，以区别于以分析学为基干的连续数学。本世纪40年代以来，受到计算机科学迅速发展的刺激，离散数学以前所未闻的势头膨胀起来，同时又推动了计算机科学的研究，并且别开生面地向社会科学领域渗透。如果说，经典的连续数学经过了几百年的发育，已形成构架完美、羽翼丰满的体系，那么，现代离散数学成为引人注目数学家族，才不过是近三十年的事情。然而，如果追溯它的历史，可以说，人类早期的数学认识是从离散对象开始的，原始数学思想的萌芽，如从计数时代算起，少说也有三千年了。所以，离散数学具有悠久的历史，是整个数学发展

的珍贵的源泉。

组合数学正是这样一门古老而又新颖的数学分支。有数学家认为：世界上还没有这样一门数学，它的历史象组合数学这样悠久，而且它对现代各门科学的应用象组合数学这样广泛而深入。人们不禁要问：什么是组合数学？它应用怎样的方法、研究什么问题？它有什么用处？

组合数学 (Combinatorial mathematics), 也叫组合学 (Combinatorics)、组合论 (Combinatorial theory)、组合分析 (Combinatorial analysis)。这个名称, 最早是德国数学家莱布尼兹 (1646—1716) 在1666年首先使用的。这里的“组合”是数学学科的专有名词, 区别于广义的“组合” (例如线性组合、工业组合等), 也区别于狭义的、作为数学名词的“组合” (Combination, 从 n 个元素中取出 k 个元素不同取法的总数)。

由于组合数学现在正在迅速发展之中, 和许多数学分支均有交叉, 所以很难下一个精确的定义, 国内外学者所下定义也不一致, 但大体来说, 组合数学是研究离散对象 (一般是有限个) 在事先给出的约束条件 (即规则) 下如何进行安排或配置的数学^[1]。如果把有限个离散对象看成一个集合, 那就是要研究按条件排成一些子集合的方法。要回答如下的问题: 一、条件是合理的, 安排是可行的, 在这种情况下, 这样的安排

有多少种？这叫做“计数”问题。二、在原来不知条件是否合理或后来条件改变了的时候，研究安排是否是可行的？这叫做“存在性”问题。三、当存在性被证明时，如何具体地设计出这种安排？这叫做“构造”问题。四、在实际应用中，往往还需要找到安排的最佳方案，这叫做“优化”问题⁽⁹⁾。组合数学可以划分成计数理论、算法理论、区组设计和图论等部分。图论的发展有独立的趋势，现在讲组合数学，有时不包括图论。

组合数学与代数学（矩阵论、近世代数等）、数论、概率统计、函数论、拓扑学、对策论、线性规划等有交叉，可以认为它是代数学的分支或边缘学科。美国代数学家柏克霍夫(G. Birkhoff)认为它主要是研究离散对象的“关系结构”，而经典抽象代数研究的是象群、环、域这样的“系统结构”。他在《代数发展的趋向》(1973)一书中说：“代数发展的主流是系统结构的研究将让位于关系结构。”按他的看法，组合数学代表了代数发展的趋向，处于主流地位。

一般数学工作者认为，组合数学属于应用数学的范畴，因为它可以应用到计算机科学、空间技术、人工智能、信息处理、编码通讯、物质结构、物理学、化学、生物学、遗传工程、实验设计、国防工业以及经济学、管理科学、生产过程控制、交通运输等几十个领域，仅在数学家族

内，它已渗透到上述交叉学科以及微分方程、数值分析、格论、模糊数学、线性代数、流形理论、拟群、射影几何等二十多个分支之中，与计算机科学相结合，与计算数学相结合，大力开展应用研究并向多学科渗透，体现了组合数学发展的倾向。它从新技术的开发中获得动力和发展空间，使自身的理论体系不断臻于完善，所以也有人认为它是计算机科学的组成部分，也是不无道理的。

组合数学的特点之一是历史性、趣味性很强。戴维德和巴顿 (Daivid & Barton) 在《组合机会》(1962) 一书的开头就举出23个数学游戏和古典问题。许多著名的难题吸引了一代又一代数学家的兴趣，如区组设计中正交拉丁方、欧拉猜想 (36军官问题)、科克曼女生问题，图论中的四色问题、货郎担问题等等，有的迄今尚未解决。它的第二个特点是涉及离散对象的问题五花八门，带来解决方法的多样性，因题而异，不拘一格。组合数学研究关系结构，是解决事理科学问题的得力工具，虽然它的理论和方法已初步形成体系，但同分析学比较起来还不够成熟。后者是研究解决物理科学问题的得力工具。这样，组合数学伴随着计算机进入社会科学领域的一些办公室，充当了秘书和参谋的角色。现代组合数学大量应用近世代数、矩阵论与数论的工具，使问题的提法和处理方法表现出极大的一般性，这

使得理论上的抽象性带来了应用上的普遍性。另外,适应计算机科学发展的现状、趋势和要求,注重方法的可行性和程序化,也是它的一个特点。

区组设计(block design),简称为BD,或称组合设计,或简称设计,就是按照规定的要求安排某些事物到一定的集合(这里称为区组)之中。例如相异代表组(system of distinct representatives),可简记为SDR。从原有的每个集合中选取一个相异元素为原有集合的相异代表组。并非任何情况下都能产生SDR的,如 $A_1 = \{1, 4\}$, $A_2 = \{1, 2, 3, 4, 5\}$, $A_3 = \{4\}$, $A_4 = \{1, 4\}$,那么从 A_1 、 A_2 、 A_3 、 A_4 中无法选出相异代表组来。于是相异代表组定理就给出在一般情况下存在SDR的充要条件:假设有 n 个集合 A_1 , A_2, \dots, A_n ,则由这些集合能产生一个SDR的充要条件是:其中任意 k 个集合($k = 1, 2, \dots, n$)的并集都至少包含 k 个相异元素。这个定理对区组设计、图论都很有用,它本身也可以认为是某一类设计的研究。

有一类区组设计的问题,可应用有限域的概念,处理有限几何、仿射平面中平行、垂直、相交诸关系的适当安排。幻方、拉丁方、罗姆方等,与我们所要讨论的平衡不完全区组设计都是设计的重要内容。

幻方(n 阶幻方或 n^2 幻方),是将一个正方形分成 n^2 个格,并填入前 n^2 个自然数的某种配

置,使其中每行、每列、两条对角线上的和均为 $\frac{1}{2}n(n^2+1)$ 。如所周知,中国文化史上具有重要影响的“洛书”是世界上三阶幻方最古老的例证⁽¹⁰⁾。在组合数学界影响较大的一本书、莱塞

(H.J.Ryser)所著的《组合数学》的第1页,开门见山地写道:“组合数学、也称为组合分析或组合学,是一门起源于古代的数学学科。据传说中国皇帝禹(约公元前2200年)在一个神龟的背上观察到纵横图:

$$\begin{pmatrix} 4 & 9 & 2 \\ 3 & 5 & 7 \\ 8 & 1 & 6 \end{pmatrix}$$

大约公元前1100年,排列在中国萌芽……”⁽¹¹⁾幻方发展的历史,可以写本厚厚的书。这里仅举一个四阶幻方的例子:多列尔幻方。多列尔是16世纪的数学家和艺术家,在他的一幅名画《郁闷》上,列出这个幻方,最下行中间两数构成1514,即是该画创作的年代:⁽¹²⁾

$$\begin{array}{cccc} 16 & 3 & 2 & 13 \\ 5 & 10 & 11 & 8 \\ 9 & 6 & 7 & 12 \\ 4 & 15 & 14 & 1 \end{array}$$

幻方有多方面的现代研究,它的一种直接的实数类比叫双随机矩阵,应用它可以找出达到最佳经济效益的多因素配置方案。除了素数幻方、级数

幻方、重幻方（不仅行、列、对角线的和一定，而且它们的积也为一定值）等之外，还向三维、多维发展，研究幻体的构作，特别应当指出的是创造了广义幻方，它是一个由非负整数（不必相异）组成的 $n \times n$ 矩阵，其原有的行之和与列之和都等于一个事先约定的数 X 。比如 $X = 15$ 的 3×3 幻方即洛书：当 $n = 1$ 时这种幻方个数为1，当 $n = 2$ 时为 $X + 1$ 。一般情形下是形如

$$\alpha_m X^m + \alpha_{m-1} X^{m-1} + \cdots + \alpha_1 X + 1$$

的多项式。此处 $m = (n-1)^2$ 。虽然公式中系数 α_i 没有明显给出，但对每个 n ，它们可由待定系数法算出，因而对较少的 X 的值，用计算机找出幻方也可确定出对所有 X 的值的幻方的个数。⁽¹⁸⁾

拉丁方是这样的配置：

A	B	C	D
B	C	D	A
C	D	A	B
D	A	B	C

其中每一字母在各行各列中都出现一次。这种单方极易构造，但如须找到正交对，就会困难得多了，如

Aa	Bb	Dc	Dd
Bc	Ad	Da	Cb
Cd	Dc	Ab	Ba
Db	Ca	Bd	Ac

两方并列，用拉丁字母大小写表示，16对Aa，

Ab, Ac, \dots , 每对只出现一次。这叫正交拉丁方。并非所有 $n \times n$ 阶 ($n \equiv 2 \pmod{4}$) 的正交拉丁方都不存在。当 $n = 6$ 时, 正如欧拉在 1781 年所猜测的那样^[14], 从 6 个不同团队中每团选出 6 种不同级别的军官, 这 36 人方阵无论怎样排, 都不可能使每行、每列中既有各团的人, 又有不同级别的官。但是欧拉猜想认定, 当 $n = 10, 14, 18, \dots$ 时 $n \times n$ 阶正交拉丁方不存在却猜错了 1960 年玻斯(R.S.Bose)等人证明欧拉猜想是错的,^[15] 是区组设计理论中一项重大成果。

正交拉丁方亦可表述为: 设 n^2 个元素, 每个既属 n 组之一, 也属 n 类之一, 且任两元素或不同组, 或不同类, 或两者均不同。要求把这 n^2 个元素安排在 $n \times n$ 矩阵中, 各行和各列分别表示各组 and 各类。拉丁方的问题在统计学、尤其是在试验设计中有重要的影响。1930 年, 英国农学家在小麦试验田里按正交设计的方法取得了很大成功, 引起了数学界的注目, 有人认为现代区组设计即发端于此。就我们所要讨论的平衡不完全区组设计而言, 与拉丁方的问题也有密切的联系。

在区组设计中一个有重大一般性的问题是把 v 元集合 X 中的元安排到指定数目的子集中去, 第 j 个子集包含 k_j 个不同元, 以便使第 i 个元在被选出的所有子集中出现 r_i 次, 并使两元组、三元组……出现一指定的次数。这可以叫做——关联系统(incidence system), 其中一基本形式是

平衡不完全区组设计 (balanced incomplete block design), 缩写为BIBD或BIB, 这一名称来自实验设计理论, 应用于统计学中。

一个BIBD是把集 X 的 v 个不同元安排到 b 个区组(子集)中, 构成一个子集族 \mathscr{B} , 使得

- (i) 每一区组恰含 k 个不同元。
- (ii) 每元恰出现于 r 个不同区组。
- (iii) 每对不同元 a_i, a_j 恰出现于 λ 个不同区组。

显然, 由定义可以推知 $v \geq k$ 。另外, 费希尔(R. A. Fisher)证明了 $b \geq v$, 称为费希尔不等式。由(ii)不难推知

$$rv = bk \quad (1)$$

$$\text{由 (iii) 也可证明 } r(k-1) = \lambda(v-1) \quad (2)$$

我们注意到, 一个BIBD有五个变量, 可以记成 (b, v, r, k, λ) -设计。它也是 t -设计中的2-设计。所谓 t -(v, k, λ)-设计 (X, \mathscr{B}) 是指由一个 v 元集 X 和 X 中某些 k 元子集(区组)族 \mathscr{B} 所组成的序对, 使得 X 中任意 t 元子集都恰含于 λ 个区组之中。 t -设计不注意BIBD中共有多少区组的数目 b 以及每元出现于不同区组的数目 r , 它重视 X 中任意 t 元(对BIBD, $t=2$)是否恰含于 λ 个区组中。 $t=2, 3, 4, \dots$, 推衍开来, 又形成一个设计体系, 2-设计显然处于这一系列的起点的重要位置上。

区组设计原来属于实验设计研究的对象, 所

22 科克曼女生问题

以它的命名和记法仍保留了这一历史的痕迹。区组(blocks)数记为 b , 元素(统计学中元素称为品种: varieties)数记为 v 。这一约定的记法在组合数学的论文中已得到公认。

三、科克曼女生问题的提出



THE UNIVERSITY OF CHICAGO

THE UNIVERSITY OF CHICAGO
LIBRARY
540 EAST 57TH STREET
CHICAGO, ILL. 60637
TEL: 773-936-5000
FAX: 773-936-5001
WWW.CHICAGO.EDU

科克曼 (Thomas Penyngton Kirkman), 1806年3月31日生于英格兰的波尔顿 (Bolton)^[16], 1895年4月3日卒于沃灵顿近郊之克洛夫特 (Croft)。他在一个没有学问的商人家庭中长大, 曾为受到较好的教育而奋斗过, 但他甚至没有受到过任何水平的数学教育。科克曼于1833年在都柏林 (Dublin) 大学获得艺术学位, 被派到英格兰教会, 成为一个教区的教区长, 达五十年之久。但是, 他个人善于思考和勤奋不懈, 使他成为具有严密性和洞察力的数学家。他很快进入当时研究的前列, 并获得了当时英国著名数学家凯莱 (Cayley)、棣莫甘 (De Morgan) 和哈密尔顿 (Hamilton) 的赞扬和友谊。1857年被选入皇家学会 (Royal Society)。科克曼还是一位优秀的语言学家和风格独特的作家。他的数学研究属于拓扑学、群论、双曲复数 (hypercomplex numbers) 以及组合数学的初期工作。他还写了关于一个非常古老的题目: 多面体。科克曼受到

哈密尔顿发现四元数的鼓舞，作出了他早期的尝试：推广到他自己命名的复四元数 (pluquaternions)。当然，在组合数学方面，由于他提出了著名的十五个女生问题，科克曼的名字已变成众所周知的了。

在19世纪中叶，英国一些数学家中展开了关于组合数学若干问题的研究，这些数学家有伍尔豪斯 (W. S. B. Woolhouse)、西尔沃斯特 (J. J. Sylvester)、斯波梯斯乌德 (W. Spottiswoode)、安斯梯斯 (R. R. Anstice) 以及科克曼、凯莱等人。他们之中有的是剑桥学者，有的彼此之间有交往，不少论文内容相关，发表在剑桥、都柏林、伦敦的两种学术刊物⁽¹⁷⁾⁽¹⁸⁾上，形成了最早的组合数学学派。

在这样的学术背景下，1850年科克曼在《女士与先生之日记》杂志上发表题为“疑问六”的文章⁽¹⁹⁾，提出了15个女学生问题：一位女教师每天带领她班上的15名女生去散步，她把她们按3人一组分成5组，问能不能作出一个连续散步7天的分组计划，使得任意两个女生曾被分到一组且仅被分到一组？也就是说，随便从15人中挑出2人，她们在一周所分成的35个小组里必在一个组中见过一面，且仅见一面。

这个饶有趣味的游戏在一些数学家的介绍、研究和推广下，很快就在许多国家里流传开来。我们先看科克曼本人在当年给出的答案，它发表

在1851年同一杂志上^[20]：

将15名女学生从1到15编号，则一周内可作如下分组：

星期日 $\{1, 2, 3\}, \{4, 8, 12\}, \{5, 10, 15\}$,
 $\{6, 11, 13\}, \{7, 9, 14\}$;

星期一 $\{1, 4, 5\}, \{2, 8, 10\}, \{3, 13, 14\}$,
 $\{6, 9, 15\}, \{7, 11, 12\}$;

星期二 $\{1, 6, 7\}, \{2, 9, 11\}, \{3, 12, 15\}$
 $\{4, 10, 14\}, \{5, 8, 13\}$;

星期三 $\{1, 8, 9\}, \{2, 12, 14\}, \{3, 5, 6\}$,
 $\{4, 11, 15\}, \{7, 10, 13\}$;

星期四 $\{1, 10, 11\}, \{2, 13, 15\}, \{3, 4, 7\}$
 $\{5, 9, 12\}, \{6, 8, 14\}$;

星期五 $\{1, 12, 13\}, \{2, 4, 6\}, \{3, 9, 10\}$,
 $\{5, 11, 14\}, \{7, 8, 15\}$;

星期六 $\{1, 14, 15\}, \{2, 5, 7\}, \{3, 8, 11\}$,
 $\{4, 9, 13\}, \{6, 10, 12\}$ 。

表2. 科克曼给女生问题作出的解(1851)

让我们回到开始时所提出的Nim游戏的制胜方案，将表2同表1进行比较，两个方案各有35个区组，它们竟是相同的！当然，表2还要讲究每天都须有1—15出现，为此在排法上与表1有别，这一点也是重要的。

对照上节 BIBD的定义，可知在科克曼女生问题原题中， $b = 35$ ， $v = 15$ ， $r = 7$ ， $k = 3$ ， $\lambda = 1$ ，因此，这一问题应当称为 $(35, 15, 7,$

3, 1) - 设计。

在这个问题中女生数目15是可以改变的, 为了满足3人一组的要求, v 应当是3的倍数; 而天数7即 r 也应作相应的改变, 于是女生问题被推广成一般性问题。这里先举9名女生在4天内的分组方案:

第1天	第2天	第3天	第4天
{1, 2, 3}	{1, 4, 7}	{1, 5, 9}	{1, 6, 8}
{4, 5, 6}	{2, 5, 8}	{2, 6, 7}	{2, 4, 9}
{7, 8, 9}	{3, 6, 9}	{3, 4, 8}	{3, 5, 7}

表3. (12, 9, 4, 3, 1)设计

如果把第1天列出的9个数字看成方阵, 那么表3的12个区组是这个方阵按三横行、三纵列和行列式展式中六个乘积的顺序排出的。

当然, 科克曼给出的解并不是他所提出问题的唯一答案, 通过调换元素命名和区组排列顺序能得到一个貌似不同的解, 但在数学上是等价的, 不认为两者间有什么区别。排除掉这种情况, 仍然可以写出不少答案来, 例如:

星期日 {1, 2, 5}, {3, 14, 15}, {4, 6, 12},
{7, 8, 11}, {9, 10, 13};

星期一 {1, 3, 9}, {2, 8, 15}, {4, 11, 13},
{5, 12, 14}, {6, 7, 10};

星期二 {1, 4, 15}, {2, 9, 11}, {3, 10, 12},
{5, 7, 13}, {6, 8, 14};

星期三 {1, 8, 10}, {2, 13, 14}, {3, 4, 7},

$\{5, 6, 9\}, \{11, 12, 15\};$

星期四 $\{1, 6, 11\}, \{2, 7, 12\}, \{3, 8, 13\},$
 $\{4, 9, 14\}, \{5, 10, 15\};$

星期五 $\{1, 7, 14\}, \{2, 4, 10\}, \{3, 5, 11\},$
 $\{6, 13, 15\}, \{8, 9, 12\};$

星期六 $\{1, 12, 13\}, \{2, 3, 6\}, \{4, 5, 8\},$
 $\{7, 9, 15\}, \{10, 11, 14\}.$

表4.15女生问题的一个解

应当说，要判断表4与表2不是等价的并不很容易。问题的关键是，总共能写出多少种不同的方案来？

西尔沃斯特在科克曼提出女生问题以后，就对这一问题提出了一个进一步的要求^[21]。他们认为这样的方案可以写出许多，如果保持每周内的安排都符合原来的规定，一周周地排下去，再加上一个新要求：任意三名女生在以后各周内都恰有（意即有且仅有）一次被分在同一组，那么能够排出的周数是与女生人数相关的——他们猜测，这样的方案可以排出 $15 - 2 = 13$ 周来！这一猜想是超越时代的，许多人都不能充分理解这一新问题有多么大的难度，后来被称为“西尔沃斯特问题”。在表2和表4中，都有 $(3, 4, 7)$ ， $(1, 12, 13)$ 等三元组，它们是“相交”的而非“相斥”的，因而，如果将表2作为第一周的安排方案，那么表4将不能作为以后12周中任何一周的方案。读者若有兴趣，不妨依表

2 作一两个“不相交”的方案，它将是对你能力、意志与耐性的一次挑战。

事实上，过了一百多年，到1974年这一问题才由德尼斯顿(R. H. F. Denniston)借助于电子计算机得到解决⁽²²⁾。表5中，15名女生分别记为 $a, b, 0, 1, 2, \dots, 12$ ；每周分组安排分别对应于 $i = 0, 1, 2, \dots, 12$ ；式中加法的结果取以13为模的同余类，即用13去除，仅取余数。

星期日 $\{i, a, b\}, \{8+i, 9+i, 12+i\},$
 $\{3+i, 7+i, 10+i\}, \{2+i, 6+i, 11+i\},$
 $\{1+i, 4+i, 5+i\};$

星期一 $\{2+i, 8+i, b\}, \{1+i, 6+i, a\},$
 $\{4+i, 7+i, 11+i\}, \{3+i, 5+i, 9+i\},$
 $\{i, 10+i, 12+i\};$

星期二 $\{11+i, 12+i, b\}, \{4+i, 10+i, a\},$
 $\{6+i, 7+i, 9+i\}, \{1+i, 2+i, 3+i\},$
 $\{i, 5+i, 8+i\};$

星期三 $\{5+i, 7+i, b\}, \{3+i, 12+i, a\},$
 $\{2+i, 9+i, 10+i\}, \{1+i, 8+i, 11+i\},$
 $\{i, 4+i, 6+i\};$

星期四 $\{4+i, 9+i, b\}, \{2+i, 5+i, a\},$
 $\{6+i, 8+i, 10+i\}, \{1+i, 7+i, 12+i\},$
 $\{i, 3+i, 11+i\};$

星期五 $\{1+i, 10+i, b\}, \{9+i, 11+i, a\},$
 $\{5+i, 6+i, 12+i\}, \{3+i, 4+i, 8+i\},$
 $\{i, 2+i, 7+i\};$

星期六 $\{3+i, 6+i, b\}$, $\{7+i, 8+i, a\}$,
 $\{5+i, 10+i, 11+i\}$, $\{2+i, 4+i, 12+i\}$,
 $\{i, 1+i, 9+i\}$ 。

表5. 西尔沃斯特问题的解(1974)

按照上述规定, 将13张表逐一写出, 共得到
 $5 \times 7 \times 13 = 455$ 个不同的三元组。如果要检验
 这些表是否算对了, 就要查一查: 1. 每天 (共
 $7 \times 13 = 91$ 天) 是否恰有15人; 2. 每周任意一对
 (共 $\binom{15}{2} = 105$ 对)女生是否恰分于一组; 3. 全
 部13周里455个三元组是否都互不相同。真要这
 样做, 恐怕要费许多小时, 还有可能搞糊涂, 看
 来检验也需要用计算机了。

注意, 三元组的总数与15取3的组合总数相
 等:

$$\binom{15}{3} = \frac{15 \times 14 \times 13}{3!} = 455$$

这不是偶然的, 这是从15个女生中任选3人分为
 一组不同分法的总数, 不存在比它更多的满足条
 件的三元组了, 因此西尔沃斯特和凯莱的猜想把
 15女生问题的方案定为13周, 即已把它定为最大
 可能的数值。

科克曼女生问题激起了兴趣的浪潮。科克曼
 本人从1847年到1891年关于斯坦纳三连系 (下节
 即叙述到)、女生问题共发表了11篇论文, 例
 如, 1862年他写了“关于15女生难题”的文章^[2],

继续这方面的研究。由于科克曼的成就，他本人也成为数学史家研究的对象，现代组合学家比格斯 (N. L. Biggs) 曾为科克曼写过一篇很长的传记^[24]。19世纪以来，不少数学家沿着这一方向前进，主要是英、德、法等国的学者作出了贡献。西尔沃斯特 (James Joseph Sylvester, 1814—1897)^[25] 是有名望的伦敦数学家，也是凯莱的好友，1892年前曾发表10篇有关论文，包括“西尔沃斯特问题”在内，推进了这一问题的研究。另一位早期研究者伍尔豪斯，在1861—1867年发表4篇论文，追踪着这一问题。

到了19世纪90年代，对三连系的研究形成了一个高峰，十四、五位数学家连续发表文章，其中穆尔 (E. H. Moore) 从1893年到1899年每年发表一篇。关于他的工作，有人曾著文介绍^{[26][27]}。

随着论文的增多，科克曼女生问题逐步普及。1892年保尔 (W. W. R. Ball) 著书《数学游戏和问题》^[28]，后译成法文；1905年易名《数学游戏和随笔》，也有法译本；1939年经考克斯特 (H. S. M. Coxeter) 修订已出第11版。它的第10章即专论女生问题。此书流传广远，影响较大。

在本节中，我们只是叙述了科克曼女生问题产生的历史和有关的某些结果。由这些史料可以引出几个在区组设计中具有重大意义的一般问题。例如，已经提到女生数目是可以改变的，它

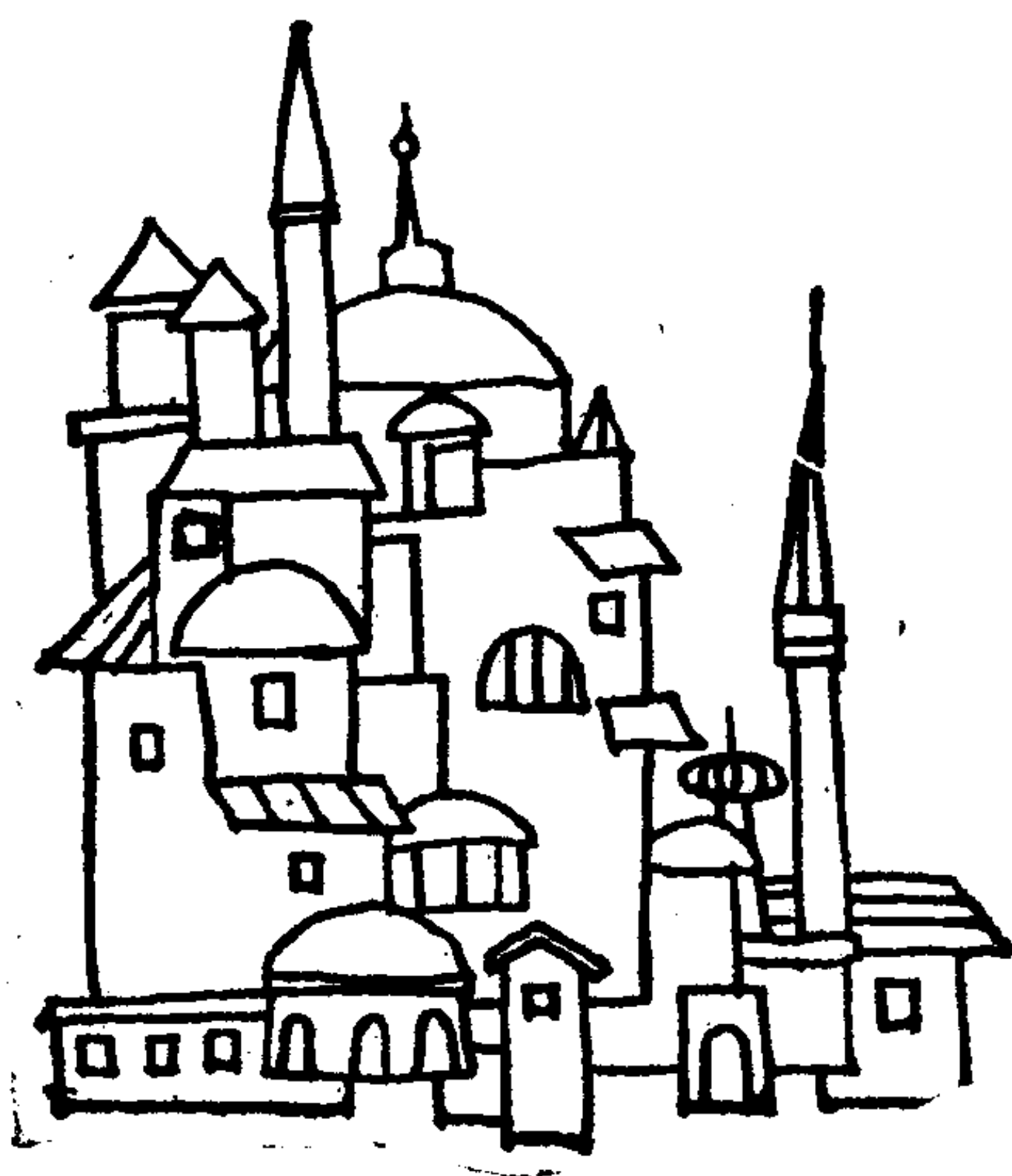
应当是3的倍数；那么进而可问：是否只要满足了这一必要条件，就一定能构造出女生的散步方案来？比如当 $v=18$ 时，是办不到的， $v=3k$

($k=1, 2, \dots$) 这一必要条件并不充分。于是，寻找并证明一般女生问题的充要条件就成为区组设计里的一个重要存在性问题了。也是过了一百多年，这个问题才获得解决，下文还要论及。

另一个重大问题是：对于任意可以构造女生散步方案的 v ，是不是总可以得到 $v-2$ 个没有相同三元组的方案来？西尔沃斯特问题到1974年才解得 $v=15$ 确实有13个方案，直到今天，这一问题距离解决还十分遥远。

显然，有必要将15女生问题及其推广形式置于一个严格的理论体系之中进行深入的讨论。上文已提及，它属于平衡不完全区组设计的典型例子。具体来说，属于带有附加条件——即“可分解”的斯坦纳三连系，或科克曼三连系。在以下的几节里引入这些概念之前，有必要介绍研究区组设计时常用的几种数学工具：矩阵论、有限域论等。

四、关联矩阵及其在区 组设计中的应用



在种类繁多的组合问题面前，数学家们需要找到这些貌似不同的问题的内在一致性，设法从已有的数学武库中找出合用的武器来，使这些问题获得一般的解决。这不是一件容易的事，它需要敏锐的观察力，甚至灵感。

先举一个简单的例子。现在有一个矩形 R ，它的高和长分别等于正整数 m 和 n 。把 R 划分成高和长也都是正整数的 t 个小矩形，按照任意选定的顺序给它们编号：1, 2, ..., t 。例如图

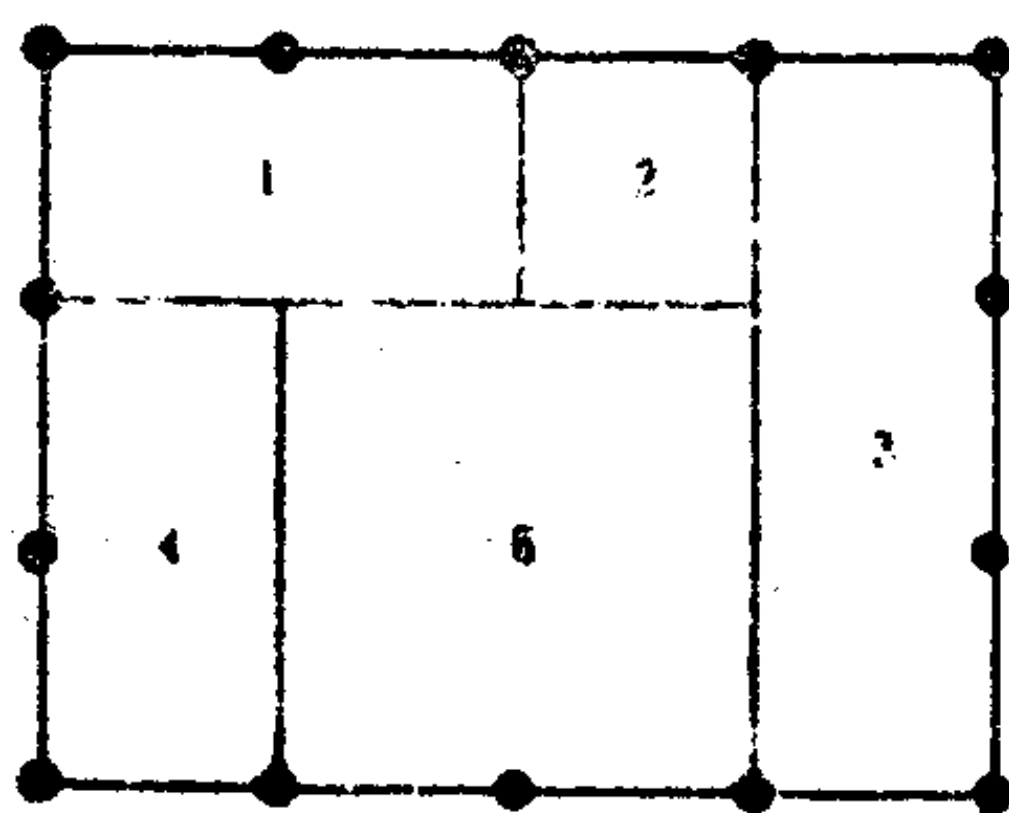


图 1 矩形 R 的划分

1 是 $m = 3$, $n = 4$, $t = 5$ 的一种情形。

数学家们想到用矩阵和矩阵乘积来表示上面所叙述的划分，这真是一件难以料想到的事。具体的做法是：设 X 是3行5列的矩阵， Y 是5行4列的矩阵，它们的元素只取0或1这两个整数。依图1，我们有：

$$X = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \quad Y = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

X 中的5列依5个小矩形的编号顺序存有它们的高度和位置的信息。例如矩形1高为1，紧接
着矩形 R 的上水平线，记作 $\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}$ 写入 X 的第1列；

矩形4高为2，靠着矩形 R 的下水平线，记作 $\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}$ 写

入 X 的第4列。这样， X 的第 i ($i=1,2,3,4,5$) 列中所有的1是相连的，其个数等于矩形 i 的高，1的位置由矩形 i 的上下位置确定，据图1 X 便被唯一地确定。类似地， Y 中的5行依序存有5个小矩形的长度和位置的信息。例如矩形3长度为1，紧靠矩形 R 的右边线，记作0001写入 Y 的第3行；矩形5长为2，左右居中，记作0110写入 Y 的第5行。这样， Y 的第 j ($j=1,2,3,4,5$) 行中所有的1是相连的，其个数等于矩形

j 的长, 1 的位置由矩形 j 的左右位置确定, 据图 1Y 便被唯一地确定。于是, 可以将矩阵 X 与 Y 相乘, 得:

$$XY = J \quad (4.1)$$

这里, J 是 3 行 4 列的、元素全为 1 的矩阵。这一结果表明矩阵的乘法可以用来存贮信息和表达图 1 所示的划分。由于矩阵运算是人们熟知的, 将它赋予某种具体的组合意义之后再大量运用这种工具, 便会得出一系列一般性的结果, 这比逐个研究各种组合现象要简便、优越得多, 所以矩阵论便在组合数学区组设计中成为一种强有力的武器。

现在引入关联矩阵的概念。设 $X = \{x_1, \dots, x_n\}$ 是一个 n 元非空集合, 称 X 为一个 n -集。又设 X_1, \dots, X_m 是 n -集 X 的 m 个子集, 它们不一定互不相同。如果当 $x_j \in X_i$ 时令 $a_{ij} = 1$, 而当 $x_j \notin X_i$ 时令 $a_{ij} = 0$, 这样得到的 m 行 n 列即 $m \times n$ 型的 $(0, 1)$ -矩阵

$$A = [a_{ij}] (i = 1, \dots, m; j = 1, \dots, n) \quad (4.2)$$

就叫做关于 X 的子集 X_1, \dots, X_m 的关联矩阵。

n -集 X 和它的 m 个子集 X_1, \dots, X_m 构成的组态 (configuration) 具有很大的普遍性, 许多组合理论问题可以归结为这种组态。在它的关联矩阵 A 中, 第 i 行表示子集 X_i , 而第 j 列则存有元素 x_j 是否属于这 m 个子集的记录, 因此 A 贮存了子集 X_1, \dots, X_m 以及元素 x_1, \dots, x_n 是否属于

这些子集的全部信息。

设 A^T 是上述 $(0, 1)$ 矩阵的转置矩阵, 则

$$AA^T = B \quad (4.3)$$

$$A^T A = C \quad (4.4)$$

分别是 m 阶和 n 阶的元素为非负整数的对称方阵, 它们的组合意义进一步展示了组态内部的结构。 B 的 (i, j) 元素 (即 i 行 j 列上的元素) 记录了 $X_i \cap X_j$ 的元素个数, 而 C 的 (i, j) 元素则记录了在 m 个子集 X_1, \dots, X_m 中有多少个同时含有 x_i 和 x_j 。仍以图 1 为例说明这个问题。

$$XX^T = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 1 \\ 1 & 3 & 3 \\ 1 & 3 & 3 \end{pmatrix} = D$$

$$X^T X = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 3 & 2 & 2 \\ 0 & 0 & 2 & 2 & 2 \\ 0 & 0 & 2 & 2 & 2 \end{pmatrix} = E$$

$$YY^T = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 2 \end{pmatrix} = F$$

$$Y^TY = \begin{pmatrix} 10010 \\ 10001 \\ 01001 \\ 00100 \end{pmatrix} \begin{pmatrix} 1100 \\ 0010 \\ 0001 \\ 1000 \\ 0110 \end{pmatrix} = \begin{pmatrix} 2100 \\ 1210 \\ 0120 \\ 0001 \end{pmatrix} = G$$

本例中 E, F 结合起来相当于 (4.3) 之 B ;
 D, G 结合起来相当于 (4.4) 之 C 。 (i, j) 位置上的元分别用 e_{ij}, f_{ij}, d_{ij} 和 g_{ij} 表示。我们有如下的解释 (X_1, \dots, X_5 依次表示图 1 中矩形 1, $\dots, 5$) :

1. 矩阵 E 的意义: 只考虑图 1 中矩形的
 高度, 矩形 X_i 占据几个单位的高度线段即是有几个元素。 $e_{11}=1$ 说明 X_1 高为 1, $e_{33}=3$ 说明 X_3 高为 3; $e_{12}=1$ 说明 X_1 与 X_2 有 1 个单位的等高处, $e_{23}=1$ 说明 X_2 与 X_3 有 1 个单位的等高处; $e_{14}=0$ 说明 X_1 与 X_4 没有等高处, $e_{25}=2$ 说明 X_2 与 X_5 有 2 个单位的等高处, 等等。

2. 矩阵 F 的意义: 只考虑图 1 中矩形的长
 度, 矩形 X_i 占据几个单位的长度线段即是有几个元素。 $f_{11}=2$ 说明 X_1 长为 2, $f_{33}=1$ 说明 X_3 长为 1; $f_{14}=1$ 说明 X_1 与 X_4 有 1 个单位的长度处于同一纵列, $f_{25}=1$ 说明 X_2 与 X_5 有 1 个单位的长度处于同一纵列; $f_{12}=0$ 说明 X_1 与 X_2 没

有任何部分处于同一纵列, $f_{ii} = 0$ 说明 X_i 与 X_i 没有任何部分处于同一纵列, 等等。

3. 矩阵 D 的意义: 用 3 条 1×4 的带子可以铺满图 1, 把占据 1, 2, 3 行的带子用元素 x_1, x_2, x_3 表示。 $d_{11} = 3$ 说明占据第 1 行 x_1 的矩形有 3 个 (X_1, X_1, X_3), $d_{12} = 1$ 说明占据第 1 行 x_1 和第 2 行 x_2 的矩形有 1 个 (X_2), $d_{23} = 3$ 说明占据第 2 行 x_2 和第 3 行 x_3 的矩形有 3 个 (X_2, X_2, X_3), 等等。

4. 矩阵 G 的意义: 用 4 条 1×3 的带子可以铺满图 1, 把占据 1, ..., 4 列的带子用元素 x_1, \dots, x_4 表示。 $g_{11} = 2$ 说明占据第 1 列 x_1 的矩形有 2 个 (X_1, X_4), $g_{44} = 1$ 说明占据第 4 列 x_4 的矩形有 1 个 (X_3); $g_{12} = 1$ 说明横跨第 1 列 x_1 和第 2 列 x_2 的矩形有 1 个 (X_1), $g_{23} = 1$ 说明横跨第 2 列 x_2 和第 3 列 x_3 的矩形有 1 个 (X_3), $g_{13} = 0$ 说明没有哪个矩形横跨第 1 列 x_1 和第 3 列 x_3 , 等等。

我们看到, 当使用关联矩阵稍加推演后, 便得到了一系列的结果, 展示了这一组态内在的关系结构, 许多细微之处, 竟是始料不及或未曾注意到的。本例较简单: 对于复杂对象运用矩阵论来处理, 其有效性就更明显了。

再举一个区组设计的实例。乒乓球队的教练要给他的 7 名运动员设计一套集训方案, 使得每三人一组, 每两人恰对阵一次 (这时第三人任裁

判)，问应当如何编组？

由于每两人须仅赛一次，共赛 $\binom{7}{2} = 21$ 次；
 每组两两对阵赛 3 次，故应分 7 组，每人在 3 组中出现。这种分法与女生问题有区别。此题用直接法来分并不困难，今编为表 6。

$\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 4, 6\}$
 $\{2, 5, 7\}, \{3, 4, 7\}, \{3, 5, 6\}$

表 6. 一个 $(7, 3, 1)$ -设计

注意到，表 6 是表 1 或表 2 的部分三元组构成的，即这个解可在 Nim 制胜方案或科克曼给出的女生分组方案之中找到。当然，编组法不唯一。一种“不费脑筋”的办法是作出如下带内切圆的正三角形，随意在 7 个交点上标出 1—7。如果有兴趣的话，不妨算一算，没有任何一个三元组相同的编组法共有多少种？

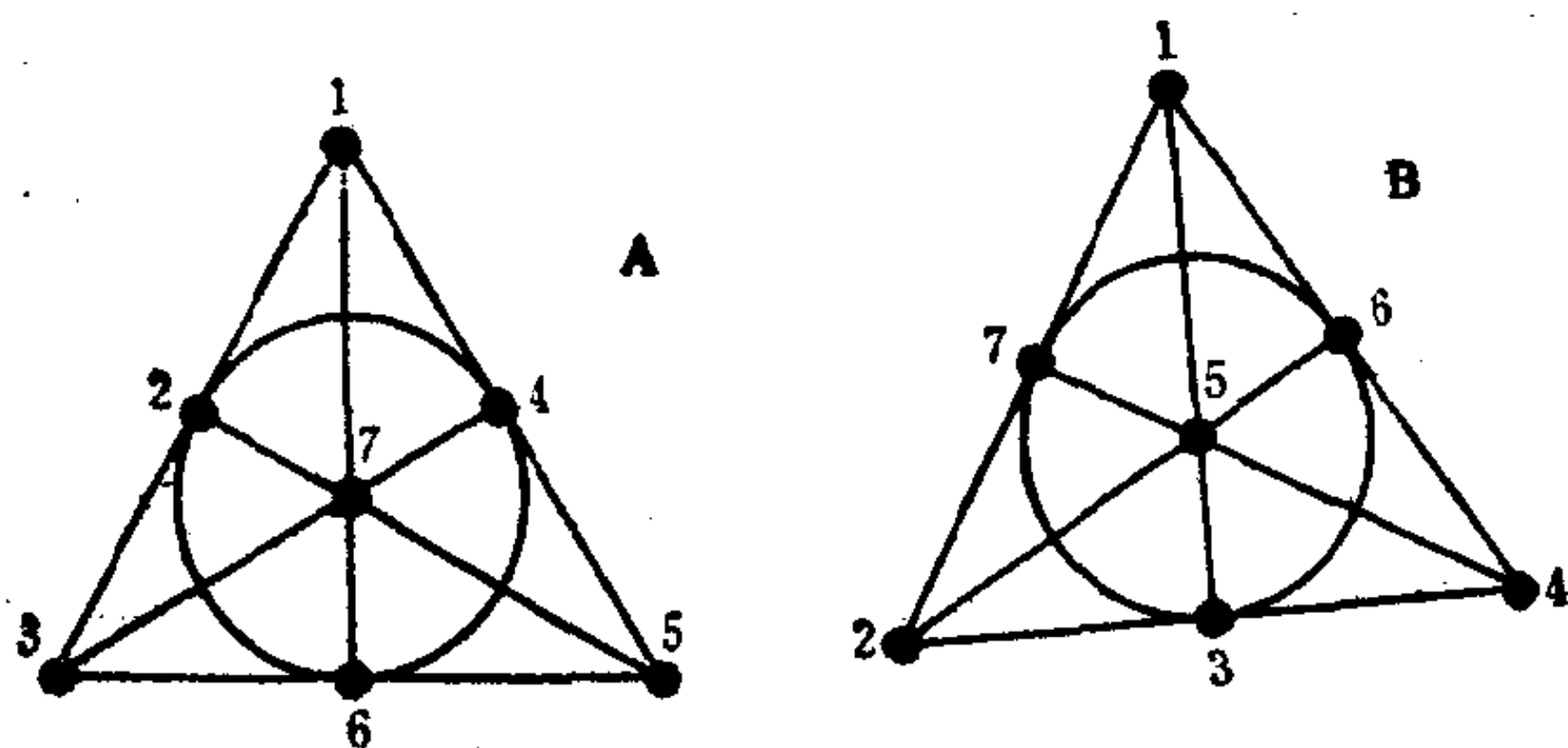


图 2 利用几何图形构造一个三连系

也可以运用关联矩阵来解决构造这类方案的问题。具体做法是：设计一个 7×7 型的 $(0, 1)$ -矩阵 A ，在它的第 1—7 行中记入表 6 的 7

个三元组的信息，例如 $\{1, 2, 3\}$ 记作 (1110000) ， $\{1, 4, 5\}$ 记作 (1001100) ，即三元组中数字所表示的位置写成1，其余位置用0填满，得：

$$A = \begin{pmatrix} 1110000 \\ 1001100 \\ 1000011 \\ 0101010 \\ 0100101 \\ 0011001 \\ 0010110 \end{pmatrix} \quad B = \begin{pmatrix} 0111000 \\ 0100110 \\ 1010100 \\ 0010011 \\ 1001010 \\ 0001101 \\ 1100001 \end{pmatrix}$$

矩阵 A 与表6、图2之 A 相一致，矩阵 B 与图2之 B 、下文的表7相一致。将1与0分别用实线和虚线连结起来，可以看出矩阵 A 是关于主对角线为对称的。能够证明，它的转置矩阵 $A^T = A$ 。这里 $v=7$ ， $k=3$ ， $\lambda=1$ 。对于一个一般的对称区组设计，它的定义是：

一个 v -集 $X = \{x_1, x_2, \dots, x_v\}$ 的 v 个子集 X_1, \dots, X_v 称为一个对称 (v, k, λ) -设计，如果下列条件得到满足：

(i) 每个 X_i 都是 X 的 k -子集 (4.5)

(ii) 每个 $X_i \cap X_j$ ($i \neq j$) 都是 X 的 λ -子集
(4.6)

(iii) 整数 v, k, λ 适合 $0 < \lambda < k < v-1$

(4.7)

我们看到，表6和表7的 $(7, 3, 1)$ -设计都是对称的区组设计。把 A 的逆矩阵 A^{-1} 记为 B ，

则有

$$AB = BA = E \quad (4.8)$$

E 是 7 阶的单位矩阵。事实上上面写出的矩阵 B 正是 A 的逆，它表示的设计如表 7 所列。图 2 之 B 与表 7 表示的一致。

{2,3,4} {2,5,6} {1,3,5} {3,6,7}
{1,4,6} {4,5,7} {1,2,7}

表 7. 一个与表 6 不同的 $(7,3,1)$ -设计

在表 6 和表 7 之中，没有任何一对三元组是相同的，因此称这两个设计是“不相交的”或“互斥的”。当然，对表 6 而言，还可以写出与它不相交的 $(7,3,1)$ -设计来，例如矩阵 B 的 7 列如果写成三元组则可得到表 8，它是 B 的转置 B^T 。

{3,5,7} {1,2,7} {1,3,4} {1,5,6}
{2,3,6} {2,4,5} {4,6,7}

表 8. 一个与表 7 有交的 $(7,3,1)$ -设计

表 8 和表 6 虽没有一对三元组是相同的，但和表 7 却有一组 {1,2,7} 相同。这一事实非常重要，下文还要专门提到。事实上早在 1850 年已证明，对于象表 6 这样的一种设计而言，只存在一种设计与它不相交，不存在第三种设计与前两者均不相交。

再考虑关联矩阵 A 和它的转置矩阵 A^T 的乘积的问题。根据对称 (v,k,λ) -设计的条件，它的关联矩阵 A 可以证明满足矩阵等式：

$$AA^T = (k - \lambda)E + \lambda J \quad (4.9)$$

这里 A 是 v 阶 $(0,1)$ -矩阵, E 为 v 阶单位矩阵, J 为 v 阶全 1 矩阵。

证明: 令 $B = AA^T = (b_{ij})_{v \times v}$, 则 b_{ij} 为矩阵 A 的第 i 行与第 j 行的内积, b_{ii} 为矩阵 A 的第 i 行中非零元素个数, 故 $b_{ii} = r$ 。 $i \neq j$ 时 $b_{ij} = \lambda$, 即第 i 行与第 j 行中对应分量都等于 1 的个数等于 λ , 说明 x_i 和 x_j 在 λ 组中同时出现。故:

$$AA^T = \begin{pmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \cdots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \cdots & r \end{pmatrix} = (r - \lambda)E + \lambda J$$

(4.9) 式对于平衡不完全区组设计 (b, v, r, k, λ) -设计也是成立的, 利用它可以证得有关的一些重要关系式。

定理: 在 (b, v, r, k, λ) -设计中, 必有 $b \geq v$
(费希尔不等式) (4.10)

证明: 由于 $k \neq v$, $r(k-1) = \lambda(v-1)$, 故 $r \neq \lambda$ 。

假定 $b < v$, 关联矩阵 A 加上元素为 0 的 $v-b$ 列形成一 $v \times v$ 的方阵 A_1 , 而且 $AA^T = A_1A_1^T$ 。故它们行列式的值有

$$\det(AA^T) = \det(A_1A_1^T) = \det(A_1)\det(A_1^T)$$

然而 A_1 至少有一列全为零, 故 $\det(A_1) = 0$ 。

$$\det(AA^T) = 0 \quad (4.11)$$

另一方面:

$$\det(AA^T) = \begin{vmatrix} r & \lambda & \lambda \cdots \lambda \\ \lambda & r & \lambda \cdots \lambda \\ \lambda & \lambda & r \cdots \lambda \\ \vdots & \vdots & \vdots \ddots \vdots \\ \lambda & \lambda & \lambda \cdots r \end{vmatrix}$$

右端行列式的第 2 列、第 3 列、…、第 v 列分别减以第 1 列得：

$$\det(AA^T) =$$

$$\begin{vmatrix} r & \lambda - r & \lambda - r \cdots \lambda - r \\ \lambda & r - \lambda & 0 \cdots 0 \\ \lambda & 0 & r - \lambda \cdots 0 \\ \lambda & 0 & 0 \cdots 0 \\ \vdots & \vdots & \vdots \ddots \vdots \\ \lambda & 0 & 0 \cdots r - \lambda \end{vmatrix}$$

把第 2 行、第 3 行、…、第 v 行加到第 1 行，得：

$$\begin{aligned} \det(AA^T) &= \begin{vmatrix} r + (v-1)\lambda & 0 & \cdots 0 \\ \lambda & r - \lambda & \cdots 0 \\ \lambda & 0 & \cdots 0 \\ \vdots & \vdots & \ddots \vdots \\ \lambda & 0 & \cdots r - \lambda \end{vmatrix} \\ &= [r + (v-1)\lambda](r - \lambda)^{v-1} \neq 0 \quad (4.12) \end{aligned}$$

(4.11) 与 (4.12) 相矛盾，故必有 $b \geq v$ 。证完。

一个对称 (v, k, λ) -设计必有 $b = v$ ，由于 $bk = vr$ ，故有 $k = r$ 。它们的任意两组都正好有 λ 个共同的元素，这一定理可以利用关联矩阵予以证明，这里省略。另外，对于任一 $X_i \in X (i = 1, \dots, v)$ ，所有 $X_j \setminus X_i (j \neq i, \text{即 } j = 1, 2, \dots, i-1, i+1, \dots, v)$ 构成一个关于 $X \setminus X_i$ 的 $((v-1),$

$(v-k), k, (k-\lambda), \lambda$ -设计；而所有 $X_i \cap X_j$ 构成一个关于 X_i 的 $((v-1), k, (k-1), \lambda, (\lambda-1))$ -设计，在第七节中将举出这两个定理的实例，并给予证明。

另外，对称 (v, k, λ) -设计的关联矩阵 A 一定是正规的，即

$$\text{定理： } AA^T = A^T A \quad (4.13)$$

证明：经过计算矩阵乘积 AA^T 的行列式的值可知

$$\det(AA^T) = \det((k-\lambda)E + \lambda J) = (k-\lambda + \lambda v)(k-\lambda)^{v-1} \neq 0 \quad (4.14)$$

因而 A 是非退化矩阵，它的逆阵 A^{-1} 存在，于是

$$AJ = kJ, \quad A^{-1}J = k^{-1}J \quad (4.15)$$

(4.9) 式两边右乘以 J ，得

$$AA^T J = (k-\lambda + \lambda v)J \quad (4.16)$$

由 (4.15)，(4.16) 可知

$$A^T J = (k-\lambda + \lambda v)k^{-1}J \quad (4.17)$$

再将 (4.17) 式两边取转置，得

$$JA = (k-\lambda + \lambda v)k^{-1}J \quad (4.18)$$

从而有

$$JAJ = (k-\lambda + \lambda v)k^{-1}vJ \quad (4.19)$$

又由 (4.15) 得

$$JAJ = kvJ \quad (4.20)$$

于是得到有意义的恒等式

$$k-\lambda = k^2 - \lambda v \quad (4.21)$$

从 (4.21)，(4.18) 式可以得到

$$JA = kJ \quad (4.22)$$

最终得到了

$$A^T A = A^{-1}(AA^T)A = (k - \lambda)E + \lambda A^{-1}JA = (k - \lambda)E + \lambda J = AA^T \quad (4.23)$$

于是式 (4.13) 得证。由于 (4.3) 和 (4.4) 对研究一个组态的内部结构是重要的, 所以 (4.13) 对研究对称 (v, k, λ) -设计甚为方便。仍以表 6 设计的关联矩阵 A 为例, 它是对称的, 故

$$A = A^T, AA^T = A^T A = A^2 = 2E + J \quad (4.24)$$

$$A^2 = \begin{pmatrix} 1110000 \\ 1001100 \\ 1000011 \\ 0101010 \\ 0100101 \\ 0011001 \\ 0010110 \end{pmatrix} 2 = \begin{pmatrix} 3111111 \\ 1311111 \\ 1131111 \\ 1113111 \\ 1111311 \\ 1111131 \\ 1111113 \end{pmatrix} = H$$

这个结果当然也可以直接算出来。事实上因为 (4.13) 适用于一切对称 (v, k, λ) -设计, 所以表 7、表 8 或据图 1 所得到的任何有区别的这类设计都可以同样算出, 主对角线为 3, 其余皆为 1 的 7 阶方阵 H 来。这时, (4.3) 和 (4.4) 所示的两个方阵 B 和 C 合而为一。本例中它们的阶数均为 7。 H 方阵的组合意义既有对 (4.3) 的解释, 又有对 (4.4) 的解释, 这里, X_1, \dots, X_7 表示表 6 中 7 个三元组, x_1, \dots, x_7 表示构成这

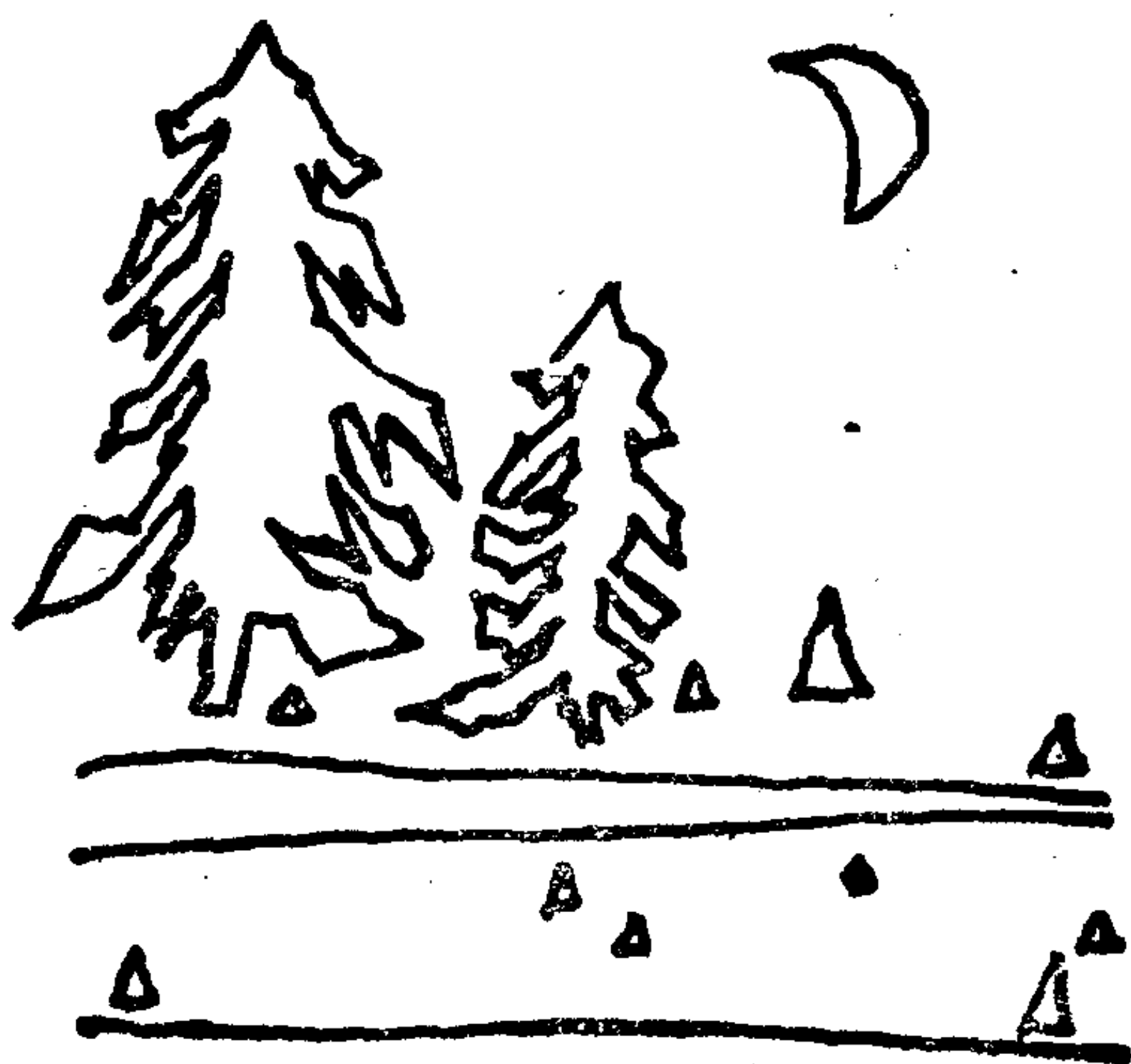
些三元组的 7 个元素 $1, \dots, 7$ 。方阵 H 的元素记作 h_{ij} 。

对 H 的解释之一：当 $i = j$ ，即在主对角线上 $X_i \cap X_j = 3$ ，说明所有 7 个子集 X_1, \dots, X_7 中均恰有 3 个元素；当 $i \neq j$ ，在主对角线外 $X_i \cap X_j = 1$ ，说明从 X_1, \dots, X_7 中任取其二，这两个三元组中恰有 1 个元素相同。

对 H 的解释之二：当 $i = j$ ， $h_{ij} = 3$ ，说明在 7 个子集 X_1, \dots, X_7 中恰有 3 个子集同时含有 x_1, \dots, x_7 中的任一元素；当 $j \neq i$ ， $h_{ij} = 1$ ，说明在 7 个子集 X_1, \dots, X_7 中恰有 1 个子集同时含有 x_1, \dots, x_7 中的任意两个元素。

关联矩阵及其应用的初步知识就介绍到这里。(0, 1)-矩阵与组合问题有着非常密切的关系：一个组合问题常常可化为 (0, 1)-矩阵的问题，而一个 (0, 1)-矩阵的组合性质往往给出某个组合的解答。关联矩阵在研究相异代表组、限位排列、区组设计、图论等许多问题时很有用，上边所举实例，已属于第六节所要讨论的“斯坦纳三连系”。表 6 的设计是一个（除 $v = 3$ 外）最小的、具有特殊性的 7 阶斯坦纳三连系。

五、有限域和有限射影 平面的应用



从形式上看，近世代数中的有限域、高等几何中的射影空间与区组设计完全没有联系，但在事实上，正象上节关联矩阵与区组设计一样，它们之间竟是密切相关的。我们首先关心的是怎样将一些数学工具同区组设计挂起钩来，从而在认识斯坦纳系、科克曼女生问题时，了解研究问题的数学观点和方法。有限域的知识更多地应用于区组设计中构造正交拉丁方；当然，在一些平衡不完全区组设计的较深刻的工作中也应用了研究正交拉丁方的成果。

所谓域 F ，是至少含有两个元素的集合，对 F 的元素定义了叫做“加法”和“乘法”的两种运算，并满足以下三个条件，这样形成的代数系统：

(i) F 的元素关于叫做“加法”的运算构成交换群，设它的单位元为 0 。

(ii) $F \setminus \{0\}$ 的元素关于叫做“乘法”的运算构成交换群，设它的单位元为 1 。

(iii) 分配律成立, 即对于 $a, b, c \in F$, 有

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$

$$(b + c) \cdot a = b \cdot a + c \cdot a.$$

全体实数、全体复数对于通常的加法、乘法都是域, 它们的元数是无限多。集合 F 的元素个数为有限时, 称为有限域。当 p 是素数, p 元集 $F = \{0, 1, \dots, p-1\}$ 对于模 p 关于“加法”和“乘法”构成域。所谓“模 n 加法”是指 n 元集合 $F = \{0, 1, \dots, n-1\}$ 中两元 a 与 b 的通常整数之和除以 n 的余数; 同样地, 所谓“模 n 乘法”是指 n 元集 F 中两元 a 与 b 的通常整数乘积除以 n 的余数 (当 $a+b, a \cdot b \notin F$ 时; 而当 $a+b, a \cdot b \in F$ 时, 这两种算法与通常的加法、乘法无异)。素数 p 元集 F 构成一个域的定理可表述成:

设 n 是不小于 2 的整数, $F = \{0, 1, \dots, n-1\}$, 那么用模 n 加法与模 n 乘法运算, 当 n 是一个素数时, F 是一个域。

进一步的结果是: 如果 F 是一个有限域, 则存在一个素数 p 和一个正整数 a , 使得 F 中的元素个数是 p^a 。对于每个素数 p 和正整数 a , 存在本质上唯一的、即同构的含有 p^a 个元素的域。

例如, 对 $p=5, a=1$, 有如下模 5 加法和乘法的结合表:

+	01234		1234
0	01234	1	1234
1	12340	2	2413
2	23401	3	3142
3	34012	4	4321
4	40123		

表8. 5元域 F 的结合表

表中数字的排列显现出一些规律性，符合区组设计中一些安排和配置的要求，于是这一方法便被移植到组合数学的领域里，较多地用于构造正交拉丁方的理论研究之中。

有 $n = p^a$ 个元素的域也叫伽罗华(Galois)域，记为 $GF(p^a)$ 。如果 $a = 1$ ， $GF(p)$ 的元素就取模 p 的完全剩余类（或称缩系）。 $0, 1, \dots, p-1$ ，这时叫做加法和乘法的域的运算，就是模 p 的普通加法和乘法。伽罗华域在近世代数中十分重要，上边的存在性定理在下文中将涉及到。根据这个定理，可知不存在元数为 $n = 6, 10, 12, 14, 15, 18, \dots$ 的伽罗华域。例如，当 $n = 6$ 时，作出模6加法和乘法的结合表（见下页表9）。

我们看到，表9中乘法结合表里出现了0元素，即不满足 $F \setminus \{0\}$ 的元素关于这种乘法运算构成交换群的条件。

伽罗华域的存在性定理对于有限射影平面。

+	012345	·	12345
0	012345	1	12345
1	123450	2	24024
2	234501	3	30303
3	345012	4	42042
4	450123	5	54321
5	501234		

表 9. 不存在元数为 6 的域

区组设计的理论同样是很重要的。

在高等几何中, 假定平面上两条平行直线相交于一个无穷远点 P_{∞} , 那么所有与这两条线平行的直线构成以 P_{∞} 为中心的平行线束, 这些直线是闭合的, 叫做扩大直线。同样, 添上这个非固有点 P_{∞} 的空间即为扩大空间。对无穷远元素和非无穷远元素不加区别的扩大空间称为射影空间, 它使“平行”消失, 出现对偶性, 使得许多命题大为简化。

所谓一个射影平面 π 是由一些称为“点”的元素和另一些称为“线”的元素组成的数学体系, 这些点和线以一定的关联关系相结合在一起。例如命题“点 P 在线 L 上”, 相当于对偶命题“线 L 通过点 P ”, 这种基本关系满足公设:

(i) π 的两个不同点在且仅在 π 的一条线上。

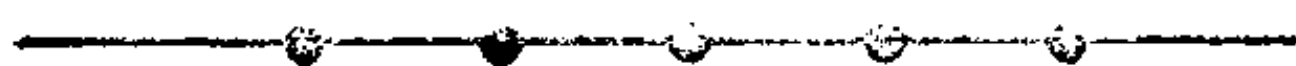
(ii) π 的两条不同线过且仅过 π 的一个点。
这里, 点和线是对偶元素, 两公设形式和内容均

是对偶的。对于欧几里得平面而言，第二个命题不常成立，因为在那里两直线若平行就没有公共点；但射影平面上两平行直线必交于 P_∞ 点使得这一命题成为一条基本公设。另外：

(iii) π 上存在 4 个点，它们中的任意 3 点都不共线。以及从以上三条推出来的：

(iv) π 上存在 4 条线，它们中的任意 3 线都不共点。

第三个命题也是一条公设，用来排除虽满足 (i) (ii) 但十分平凡的退化情况。例如：



这里只有画出来的点叫做“点”，“线”上其他几何点不是射影平面的点元素。

只含有限个点的射影平面称为有限射影平面。一般说来，一个有限射影平面可以认为是某一种区组设计，它把元素称为点的有限集合分成一些称为线的子集合，在满足上述 (i) (ii) (iii) 的条件下形成一种安排或配置。因而，它在组合数学中非常重要，在对正交拉丁方以及对称平衡不完全区组设计 (v, k, λ) 组态的讨论中它将起主要作用。如果在有限射影平面 π 的一条线 L 上总共有 $n+1$ 个点，则称正整数 n 为 π 的阶，它是 π 的基本不变量。

定理：设 P, P' 是射影平面 π 上两个不同的点， L, L' 是 π 上两条不同的线。则分别有 (a) L

上的点的集合到 L' 上的点的集合之上的一一映射, (b) 通过点 P 的线的集合到通过点 P' 的线的集合之上的一一映射, 以及 (c) L 上的点的集合到通过 P 的线的集合之上的一一映射。

证明: π 上通过两不同的点 P 和 Q 的唯一确定的线记作 PQ 。先证 π 上必有一点 O , 它既不在线 L 上, 也不在线 L' 上。假定不存在这样的点 O , 那么 π 上所有的点都在 L 和 L' 上。根据公设 (iii), 必有点 A 和 B 在 L 上, 点 C 和 D 在 L' 上, 而且这 A, B, C, D 中任意 3 点都不共线, 由此可知线 AC 和 BD 的交点既不在 L 上又不在 L' 上, 即是点 O 。现在来证 (a): 对 L 上任意一点 E , 线 OE 与线 L' 相交于唯一确定的一点 E' , 于是建立了一个把 E 映为 E' 的映射, 易见这个映射是 L 上点的集合到 L' 上点的集合之上的一一映射。用同样的方法可以建立 (a) 的对偶命题 (b) 的一一映射。另外, 如果 O 是不在 L 上的一点, 易知有 L 上的点的集合到通过 O 的线的集合之上的一一映射; 如果 O 是 L 上的一点, 根据 (b) 所述的一一映射的存在, 上述断言也是成立的, 这就证明了 (c) 所述的一一映射存在。

上述证明已指出, π 的每一条线上至少有 3 个不同的点, 通过 π 的任一点至少有 3 条不同的线。也就是说, 有限射影平面的阶数 n 最小值是 2。一般说来有:

定理: 设 π 是 n 阶有限射影平面, 则在 π 的每

一条线上点的个数以及通过每一点的线的条数都是 $n+1$ ，而且 π 一共有 n^2+n+1 个点和 n^2+n+1 条线。

证明：根据有限射影平面阶的定义和上述一一映射定理，易知 π 上每一条线上点的个数等于通过每一点的线的条数，都等于 $n+1$ 。设 O 是 π 上一点，则恰有 $n+1$ 条线通过点 O ，而且每条线上除 O 之外正好还有几个点，所以 π 上总共有 $1+n(n+1)=n^2+n+1$ 个点。根据上述一一映射定理或对偶性可知， π 上共有 n^2+n+1 条线。

这个定理表明，有限射影平面 π 如果存在，它的阶数 n 每加1时， π 上的点和线的数目增加 $2(n+1)$ ，例如从2阶变为3阶， π 上共增6点6线；从7阶变为8阶， π 上共增16点16线，等。

最小的2阶射影平面共有7个点元素，其中每3个都恰在一条线上，称为3-子集，共有7条线，而且其中每3条线都过同一点，即任3个子集的交集都恰有1个元素。这样的设计对我们已不陌生，在Nim制胜方案（表1）、科克曼15个女生问题的解（表2）中挑出含有1, ..., 7元素的那些三元组，恰为二阶射影平面。表6、表7、表8虽然在形式上有别，只是元素和子集的标号不同而已，它们是同构的，这样的组态可以不加区别。例如对图2的B，可以用一个置换 φ 把它变为图2之A，这种对应实际上就是对图B的7个点元素重新标号。如果用 x_1, x_2, \dots, x_7 标

记，它们的形式上的差别就会消失，这里7个元素与顺序无关。

为了介绍有限射影平面存在性和不存在性定理，承续上文伽罗华域的存在性定理，这里不加证明地引入与拉丁方有关的两个定理作为过渡：

$$\varphi$$

1	→	1
7	→	2
2	→	3
3	→	6
6	→	4
4	→	5
5	→	7

定理：设 $n = p^\alpha$ ，其中 p 是素数， α 是正整数，则当 $n \geq 3$ 时，一定存在一个 $n-1$ 阶拉丁方的完备正交组①。

定理：设 $n \geq 3$ ，可以构造 n 阶射影平面的充分必要条件是可以构造完备的 n 阶拉丁方的正交组。

于是我们得到有限射影平面的存在性定理，它是上边两定理的推论：

定理：设 $n = p^\alpha$ ，其中 p 为素数， α 为整数，则必存在 n 阶有限射影平面。

这个定理指出存在无限多个有限射影平面，而对于不等于 p^α 的那无限多个整数中是否仍有可以构成有限射影平面的阶数则未置一词。于是有明确的有限射影平面的不存在定理 (Bruck-Ryser 定理)：

定理：当 $n \equiv 1$ 或 $2 \pmod{4}$ 且 n 的无平方因

①关于拉丁方的有关内容可参阅文献[11], 61—73。

子部分至少有一个素因子 $p \equiv 3 \pmod{4}$ 时, n 阶有限射影平面不存在。

所谓“无平方因子部分”指 n' , 满足 $n'd = n$, d 是能整除 n 的最大的平方数, 如果 $d = 1$, 那就表明 n 无平方因子。这个定理指出有无限多个 n , 当满足定理条件时即排除了 n 阶射影平面存在的可能, 如当素数 $p \equiv 3 \pmod{4}$ 时就不存在 $n = 2p$ 阶的射影平面: 6, 14, 22, 38, 46, 54, ……等。如果把上述两个定理确认的存在和不存在的射影平面的阶数从自然数里筛掉, 仍然留下来无限多正整数处于归属不明的状态, 迄今为止还没有解决这一问题, 成为当今组合数学一大悬案。有兴趣的读者, 不妨利用计算机编一个不太复杂的程序, 把这些待定性的正整数打印出来一部分, 看看都是些什么数。第一个未解决的情况是 $n = 10$, 人们不知道有没有 10 阶有限射影平面, 更不要说对 10 后面那无限多排着队待定性的数该怎么办了。

在本节的最后, 让我们回到对称平衡不完全区组设计 (v, k, λ) -组态, 已知它的关联矩阵是正规的, 并且等价于一个当 $b = v$, $r = k$ 时的 (b, v, r, k, λ) 组态, 于是有:

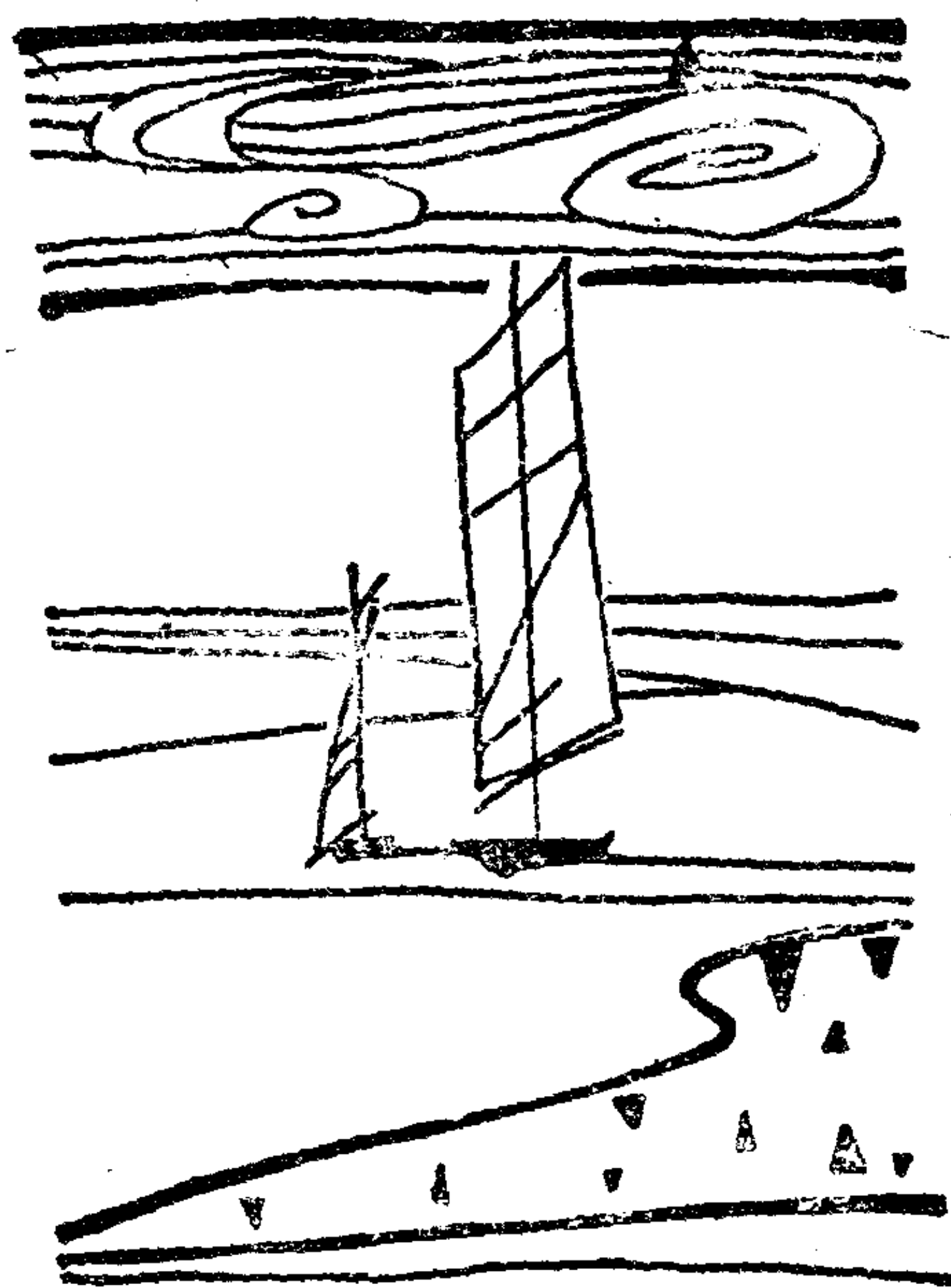
定理: 一个 n 阶有限射影平面等价于一个参数 $v = n^2 + n + 1$, $k = n + 1$ 和 $\lambda = 1$ 的 (v, k, λ) -组态。

这个定理确认了 (v, k, λ) -组态与 n 阶有限射

影平面存在性的关系，它没有告诉我们凡存在的
是否都是唯一的。进一步的研究表明，当 $n =$
 $2, 3, 4, 5, 7, 8$ 时的射影平面是唯一的，迄今为止
人们知道的也就是这些。当 $n > 8$, $n = p^\alpha$ (p 为素
数, α 为整数) 时是否唯一，就连当 $n = 9$ 时有几个
不同构的射影平面也不清楚。在人们的知识背囊
里，与射影平面相关的只有 $(7, 3, 1)-$, $(13, 4, 1)-$,
 $(21, 5, 1)-$, $(31, 6, 1)-$, $(57, 8, 1)-$, $(73, 9, 1)-$ 这
六个设计，要获得进一步的知识，还要走很远的
路程。

人类犀利的、势如破竹的认识能力在区组设
计的巨大结构面前遇到了似乎是难以逾越的障
碍，每当智慧费力地前进一步，就有十个新问题
应运而生，数学猜想将超越时代给人们以新的希
望。这样看来，问题的特殊困难性似乎并非完全
出自问题本身，而是蕴含于人类智慧矛盾的属性
之中。

六、斯坦纳系和斯坦纳 三连系



在第二节中我们曾通俗地介绍了平衡不完全区组设计(balanced incomplete block design)即 BIBD, 以后文中又涉及到它的某些性质, 这里予以重新表述和归纳:

设 X 是元素为 x_1, x_2, \dots, x_v 的 v -集, X_1, X_2, \dots, X_b 是 X 的 b 个不同的子集, 满足:

- (i) 每个 X_i 是 X 的 k -子集,
 - (ii) X 的每个 2-子集恰是 b 个集合 X_1, X_2, \dots, X_b 中 λ 个集合的子集,
 - (iii) 整数 v, k, λ 满足 $0 < \lambda, k < v-1$,
- 那么就称这些子集是一个 BIBD 或 (b, v, r, k, λ) -设计。

设 $x \in X$, x 恰属于 b 个子集 X_1, X_2, \dots, X_b 中的 r 个, X 中 v 个元除 x 外共 $v-1$ 个元都同 x 构成 2-子集。由 (i), 这 $v-1$ 个 2-子集在 b 个集合 X_1, X_2, \dots, X_b 中出现了 $r(k-1)$ 次; 由 (ii), 这 $v-1$ 个 2-子集在 b 个子集 X_1, X_2, \dots, X_b 中出现了 $\lambda(v-1)$ 次, 显然两者应当相等,

于是有:

$$r(k-1) = \lambda(v-1) \quad (6.1)$$

r 是 BIBD 的一个不变量, 它是每一个元素在子集 X_1, X_2, \dots, X_b 中出现的次数, 所以叫重复数。由于每个子集有 k 个元, 共 b 组, bk 是元素出现的总数; 又由于 v 个元素中的每一个在这 b 组中正好出现 r 次, vr 是出现的总数, 显然两者应当相等, 于是有:

$$bk = vr \quad (6.2)$$

我们已叙述了费希尔不等式的证明过程:

$$b \geq v \quad (4.10)$$

在对称的 (v, k, λ) -设计中上式取等号, 又据 (6.2) $k = r$, 这样 (b, v, r, k, λ) -设计的记法就可以省掉 b 和 r 而写成 (v, k, λ) -设计了。这五个基本参数之间的关系由 (6.1)(6.2)(4.10) 等确定。这样还是不够充分的, 区组设计研究这类组态的中心任务之一就是确定这五个基本参数值的精确范围, 今天它仍是一个没有完全解决的领域。

下面给出 (v, k, λ) -设计及其关联矩阵的两个例子。

$X_1 = \{1, 2, \dots, 8\}$, 设它的关联矩阵为 A_1 , 则一个 $(8, 4, 3)$ -设计为表10所示。

$\{1, 2, 3, 4\} \{1, 2, 7, 8\} \{1, 3, 6, 8\} \{5, 6, 7, 8\}$

$\{3, 4, 5, 6\} \{2, 4, 5, 7\} \{1, 4, 6, 7\} \{1, 2, 5, 6\}$

$\{1, 3, 5, 7\} \{2, 3, 5, 8\} \{3, 4, 7, 8\} \{2, 4, 6, 8\}$

$\{1, 4, 5, 8\} \{2, 3, 6, 7\}$

表10. 一个 $(8, 4, 3)$ -设计

$$A_1 = \begin{pmatrix} 11110000 \\ 11000011 \\ 10100101 \\ 00001111 \\ 00111100 \\ 01011010 \\ 10010110 \\ 11001100 \\ 10101010 \\ 01101001 \\ 00110011 \\ 01010101 \\ 10011001 \\ 01100110 \end{pmatrix}$$

$X_2 = \{0, 1, \dots, 8\}$, 设它的关联矩阵为 A_2 , 则一个 $(9, 4, 3)$ -设计为表11所示。

$\{0, 1, 2, 4\} \{1, 2, 3, 5\} \{2, 3, 4, 6\} \{3, 4, 5, 7\}$
 $\{4, 5, 6, 8\} \{0, 5, 6, 7\} \{1, 6, 7, 8\} \{0, 2, 7, 8\}$
 $\{0, 1, 3, 8\} \{0, 1, 4, 6\} \{1, 2, 5, 7\} \{2, 3, 6, 8\}$
 $\{0, 3, 4, 7\} \{1, 4, 5, 8\} \{0, 2, 5, 6\} \{1, 3, 6, 7\}$
 $\{2, 4, 7, 8\} \{0, 3, 5, 8\}$

表11. 一个 $(9, 4, 3)$ -设计

$$A_1 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

如果将 $(0, 1)$ -矩阵中的1连结起来, 或者想象将矩阵卷成筒状使它上下、左右相连, 则可以清楚看出它们排列的规律。

由(6.1)、(6.2)式可知:

$$r = \frac{\lambda(v-1)}{k-1} \quad (6.3)$$

$$b = \frac{\lambda v(v-1)}{k(k-1)} \quad (6.4)$$

因此(6.1)、(6.2)式等价于以下两个同余式:

$$\lambda(v-1) \equiv 0 \pmod{k-1} \quad (6.5)$$

$$\lambda v(v-1) \equiv 0 \pmod{k(k-1)} \quad (6.6)$$

(6.5)、(6.6)是 (v, k, λ) -设计存在的必要条件, 这两个同余式是否也是设计存在的充分条件呢? 这个问题纠缠了组合数学家们很长一段时间。

当 $k=1$ 时, 由 BIBD 的定义知道只能有 $\lambda=0$, $r=1$, 而由 (6.2) 式又有 $b=v$, 于是, (v, k, λ) -设计恰好是 X 的全部 1-子集; 当 $k=2$ 时, 同样知道只能有 $\lambda=1$, 而由 (6.1)、(6.2) 式又有 $r=v-1$, $b=v(v-1)/2 = \binom{v}{2}$, 于是 (v, k, λ) -设计恰好是 X 的全部 2-子集。前者 $\lambda=0$, 属 BIBD 的退化现象。为避免这种情况出现, 已在定义中加进一条 (iii), 把它排除于 BIBD 之外。后者也十分平凡, 没有什么值得研究的。

于是, 自然轮到讨论 $k=3$ 时的情况了。这时 (6.5)、(6.6) 式变为:

$$\lambda(v-1) \equiv 0 \pmod{2} \quad (6.7)$$

$$\lambda v(v-1) \equiv 0 \pmod{6} \quad (6.8)$$

特别地, 当 $\lambda=1$ 时, 上两式可合写于一式

$$v \equiv 1 \text{ 或 } 3 \pmod{6} \quad (6.9)$$

这样, 一般地称 $(v, 3, \lambda)$ -设计为三元系或三连系, 称 $(v, k, 1)$ -设计为斯坦纳系, 称 $(v, 3, 1)$ -设计为斯坦纳三元系或斯坦纳三连系,

它们是BIBD中区组最小、最基本、最重要的研究对象。

如果单独给斯坦纳三连系 \mathcal{S} 下定义,即可说 \mathcal{S} 是定义在 v 元集 X 上的 b 个3-子集,使得 X 的每一个2-子集同在一个且仅在一个三元组中。 v 阶斯坦纳三连系记作 $\text{STS}(v)$ 或 $S(v)$ 。若按 t -设计的记法, $t-(v,k,1)$ 即斯坦纳系,记作 $S(t,k,v)$,这时三连系又记作 $S(2,3,v)$ 。

斯坦纳三连系 $S(3)$ 只有一个三元组 $\{1, 2, 3\}$,属于退化的情况,不予研究;最小的是 $S(7)$,在表6, 7, 8中已熟知。其次是表3的 $S(9)$,表1, 2的 $S(15)$,也就是说,九个和十五个女学生问题的解构成一个9阶和15阶的斯坦纳三连系。现在再给出13阶的斯坦纳三连系 $S(13)$ 和它的关联矩阵 A 。

$$X = \{1, 2, \dots, 12, 0\}$$

$$\{1, 3, 9\} \{2, 4, 10\} \{3, 5, 11\} \{4, 6, 12\}$$

$$\{0, 5, 7\} \{1, 6, 8\} \{2, 7, 9\} \{3, 8, 10\}$$

$$\{4, 9, 11\} \{5, 10, 12\} \{0, 6, 11\} \{1, 7, 12\}$$

$$\{0, 2, 8\} \{2, 5, 6\} \{3, 6, 7\} \{4, 7, 8\}$$

$$\{5, 8, 9\} \{6, 9, 10\} \{7, 10, 11\} \{8, 11, 12\}$$

$$\{0, 9, 12\} \{0, 1, 10\} \{1, 2, 11\} \{2, 3, 12\}$$

$$\{0, 3, 4\} \{1, 4, 5\}$$

表12. 一个 $S(13)$

(13, 26, 6, 3, 1)-设计

A=

1	0	1	0	0	0	0	0	1	0	0	0	0
0	1	0	1	0	0	0	0	0	1	0	0	0
0	0	1	0	1	0	0	0	0	0	1	0	0
0	0	0	1	0	1	0	0	0	0	0	1	0
0	0	0	0	1	0	1	0	0	0	0	0	1
1	0	0	0	0	1	0	1	0	0	0	0	0
0	1	0	0	0	0	1	0	1	0	0	0	0
0	0	1	0	0	0	0	1	0	1	0	0	0
0	0	0	1	0	0	0	0	1	0	1	0	0
0	0	0	0	1	0	0	0	0	1	0	1	0
0	0	0	0	0	1	0	0	0	0	1	0	1
1	0	0	0	0	0	1	0	0	0	0	1	0
0	1	0	0	0	0	0	1	0	0	0	0	1
0	0	0	1	1	0	0	0	0	0	0	0	0
0	0	1	0	0	1	1	0	0	0	0	0	0
0	0	0	1	0	0	1	1	0	0	0	0	0
0	0	0	0	1	0	0	1	1	0	0	0	0
0	0	0	0	0	1	0	0	1	1	0	0	0
0	0	0	0	0	0	1	0	0	1	1	0	0
0	0	0	0	0	0	0	1	0	0	1	1	0
0	0	0	0	0	0	0	0	1	0	0	1	1
1	0	0	0	0	0	0	0	0	1	0	0	1
1	1	0	0	0	0	0	0	0	0	1	0	0
0	1	1	0	0	0	0	0	0	0	0	1	0
0	0	1	1	0	0	0	0	0	0	0	0	1
1	0	0	1	1	0	0	0	0	0	0	0	0

$S(13)$ 的矩阵 A 中如用箭头把所有的 1 顺序连结起来, 可以看出这个设计分为上下两部分, 配置的规律一目了然。

一个斯坦纳三连系 \mathscr{S} 内含有 $\binom{v}{2} = \frac{1}{2}v(v-1)$ 个 X 中的元素对, 每对恰在 \mathscr{S} 中的一个三元组中出现; 而 \mathscr{S} 中每个三元组 $\{x_1, x_2, x_3\}$ 含有 X 中的 3 个元素对, 即 x_1 与 x_2 , x_2 与 x_3 , x_1 与 x_3 。于是, \mathscr{S} 的 b 个三元组共含 $3b$ 个 X 的元素对:

$$3b = \frac{1}{2}v(v-1) \text{ 或 } b = \frac{1}{6}v(v-1) \quad (6.10)$$

这表明斯坦纳三元系中三元组的个数 b 依赖于 v , 或 b 是 v 确定的。那么, 须进而确定能构成斯坦纳三连系的那些 v 的数值, 今设任一元 $x \in X$, x 与 X 中其他 $v-1$ 元构成 $v-1$ 个元素对。

\mathscr{S} 中含 x 的一个三元组里包括含 x 的两个元素对, 因此, \mathscr{S} 中含 x 的三元组共有 $\frac{1}{2}(v-1)$ 个,

即 X 的每一元恰在 $r = \frac{1}{2}(v-1)$ 个三元组中。

r 必须是一个正整数, 由此式可知 v 必须是一个奇数。另一方面, 由 $b = \frac{1}{6}v(v-1)$ 必是正整数可知, 3 能整除或者 v , 或者 $v-1$;

1. 若 $3 \mid v$, 则对某正整数 k , 有 $v = 3k$ 成立, v 须为奇数, k 必为奇数, 故对某整数 n ($n = 0, 1,$

2, …) 有 $k = 2n + 1$ (或 $k = 2n - 1$, 对 $n = 1, 2, \dots$), 于是得到:

$$v = 6n + 3 \text{ 或 } v \equiv 3 \pmod{6} \quad (6.9a)$$

2. 若 $3 \mid (v - 1)$, 则对某正整数 k , 有 $v = 3k + 1$ 成立, v 须为奇数, k 必为偶数, 故对某整数 $n (n = 0, 1, 2, \dots)$ 有 $k = 2n$, 于是得到:

$$v = 6n + 1 \text{ 或 } v \equiv 1 \pmod{6} \quad (6.9b)$$

经过以上简单的讨论, 可得:

定理: 存在一个 v 阶斯坦纳三连系的必要条件是: 对某个非负整数 n 有 $v = 6n + 1$ 或 $v = 6n + 3$ (或: v 对模 6 与 1 或 3 同余: $v \equiv 1, 3 \pmod{6}$).

舍去 $v = 1$, 可能构成斯坦纳三连系的前边几个 v 值为 3, 7, 9, 13, 15, 19, 21, 25, 27, 31, …

定理的条件对构造一个 $S(v)$ 既是必要的, 也是充分的, 这是 1847 年科克曼在“关于一个组合问题”⁽³¹⁾ 中首先提出并证明的。在英国, 1844 年较早提出组合分析问题开始研究的有西尔沃斯特和伍尔豪斯⁽³²⁾⁽³³⁾。1850 年数学家、天文学家凯莱 (Arthur Cayley, 1821—1895)⁽³⁴⁾ 著文“关于七与十五物的三元排列”⁽²⁹⁾, 他从 1863 年起直到去世都在剑桥大学工作, 是一位高产的数学家, 曾在 14 年中写过 300 篇论文, 是素负盛望的剑桥学者。他在这篇文章里证明了对一个 $S_1(7)$, 只存在另一个 $S_2(7)$ 与 $S_1(7)$ 不相交。接着, 斯波梯斯乌德和安斯梯斯讨论了“关于一个组合问题”⁽³⁵⁾⁽³⁶⁾。

另一方面，在欧洲大陆上，1853年斯坦纳提出了后来以他的名字命名的三连系存在问题⁽³⁷⁾。他并不知道科克曼的工作，在研究四次曲线的两切线问题时遇到了这个组合问题，在两页的论文中提出了这种三连系存在的必要条件 $v \equiv 1, 3 \pmod{6}$ 对于它的存在是否也是充分的。斯坦纳 (1796—1863)⁽³⁸⁾ 出身于瑞士的一个小农场主和小商人家庭，没有受过什么教育，直到14岁还不会写字。但他天资聪颖，谙于计算，18岁离家求学，1822年就读于柏林大学，1834年成为该校教授。50年代时，他已是声名卓著的几何学家，他提出的85个“问题和定理”，直到本世纪还有人在深入研究。由于斯坦纳影响大，经他一提倡，这一组合问题引起了注意，克劳森⁽³⁹⁾ 和黎斯⁽⁴⁰⁾ 先后发表文章，后者解决了斯坦纳的这一问题，并冠以斯坦纳的名字，以后“斯坦纳系”和“斯坦纳三连系”便流传开来，变成了约定俗成的数学专名，科克曼的名字反而不为许多人所知了。

关于斯坦纳三连系的存在性定理确切指出了 v 应具备什么条件才能构成一个 $S(v)$ ，这仅仅是指 $k=3$ ， $\lambda=1$ 时的情况。经过一百多年的探索，直到1961年，哈纳尼 (H. Hanani) 证明了⁽⁴¹⁾ 对于正整数 λ ，三连系 $(v, 3, \lambda)$ 存在的必要条件 (6.7)、(6.8) 是充分的，他甚至证明了四连系 $(v, 4, \lambda)$ 存在的必要条件 (6.5)、(6.6) 也是充分

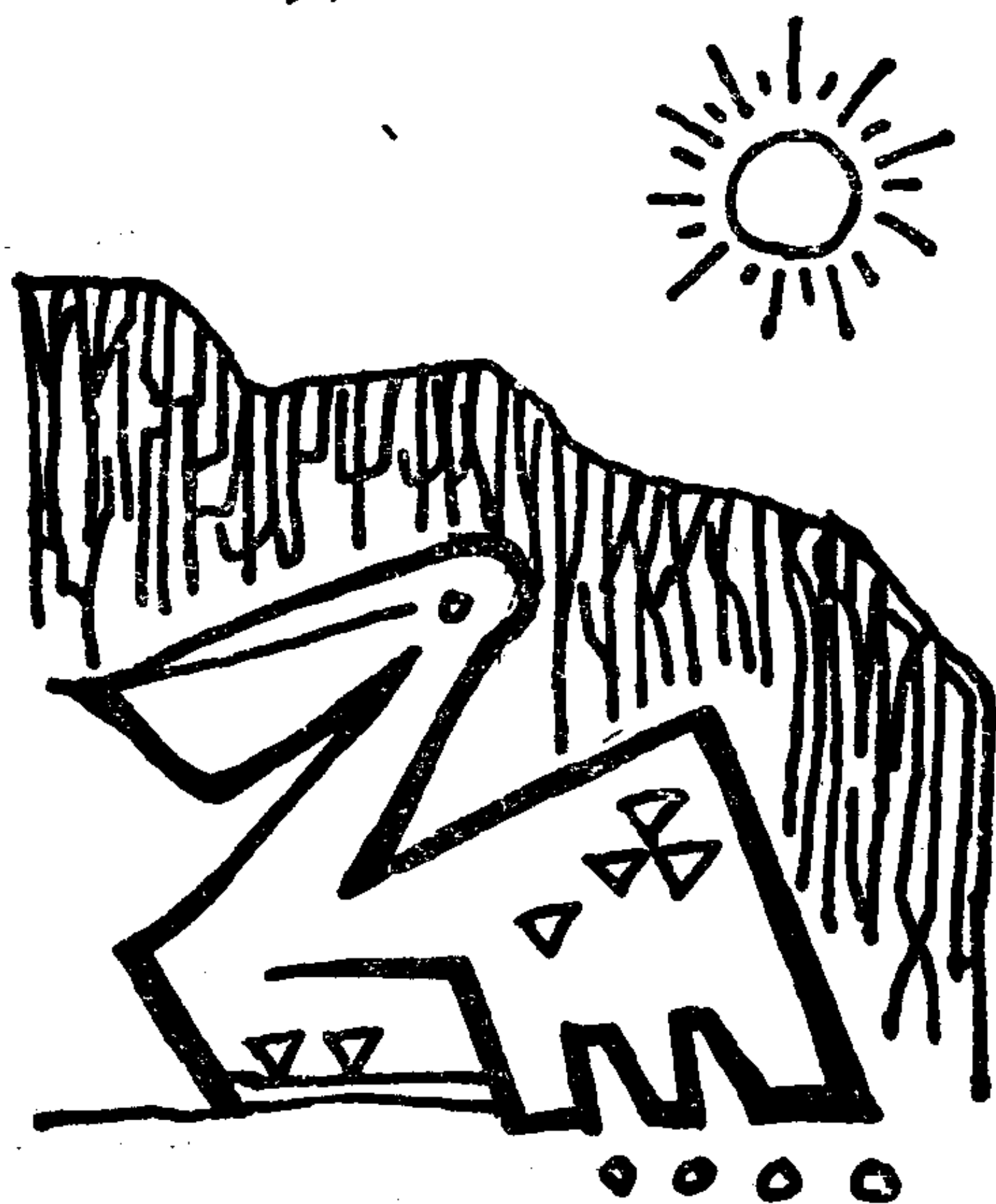
的。应当说，哈纳尼在这个问题上跨出了两大步。

但是，当 $k \geq 5$ 时，问题变得更加复杂起来，对每个超过 4 的 k 值都有着虽满足 (6.5)、(6.6) 式但相应的 (v, k, λ) -设计却不存在的 (v, λ) 数值组。于是，人们退一步提出了以下的猜想：对于给定的 k ，除去有限对数值 (v, λ) 之外，(6.5)、(6.6) 式是 (v, k, λ) -设计存在的充分条件。

1975 年，威尔逊 (Richard M. Wilson) 证明了这个猜想^[2]，他的结论是：对给定的正整数 $k \geq 5$ ，除去有限对正整数 (v, λ) 以外， (v, k, λ) -设计存在的充分必要条件是 $v \geq k$ 且 (6.5)、(6.6) 式成立。

至此，经过了自 1844 年伍尔豪斯提出问题以来的一百三十多年之久的奋斗，人们终于取得了这一类设计存在性的基本解决。

七、斯坦纳三连系和 斯坦纳系的构造 方法



在研究区组设计的一些问题时，往往需要自己动手，去具体设计一些组态，这样才能体会出创作的甘苦，感性地接触构造的规律。事实上，许多组态的存在性问题，可以随着构造的完成而获得解决。

当你构造出一个斯坦纳三连系时，比如 $S(13)$ ，首先想判断它是不是与已知的同构。一般说来，设 A_1, A_2 是两个 (b, v, r, k, λ) -组态的关联矩阵，如果存在 b 阶置换方阵 P 和 v 阶置换方阵 Q ，使得

$$A_1 = PA_2Q \quad (7.1)$$

成立，则称这两个组态是同构的。对于参数组 b, v, r, k, λ 而言，同构的 (b, v, r, k, λ) -组态可以不加区别。前边已经述及，同构的两个组态可以通过调换元素和子集的命名标号而变成同一个。

区组设计的构造方法有许多种，主要是直接法和递归法。直接法对一些特殊的变量，例如当

元数 v 为素数幂时, 使用有限域、有限射影平面或同余, 已为前文所述。当然, 早期的构造、阶数较小的构造也主要靠直接法。我们甚至可以用计算机来设计一个 $S(v)$, 关键在构造的方法已知, 并且运算是可行的。波斯在1939年以一篇47页的文章论述了“对称循环差法”, 或简称“混合差法”^[43]。

第四节我们曾提到差集 $X \setminus X_i$ 和交集 $X_j \cap X_i$ 构成新的组态的两个定理, 这里首先予以证明。

定理: 如果 X_i ($i=1, \dots, v$) 是关于集合 $X = \{x_1, \dots, x_v\}$ 的对称的 (v, k, λ) -组态, 则对于其中任一 X_i , 下列 $v-1$ 个区组: $X_1 \setminus X_i, X_2 \setminus X_i, \dots, X_{i-1} \setminus X_i, X_{i+1} \setminus X_i, \dots, X_v \setminus X_i$ 构成一个关于集合 $X \setminus X_i$ 的 $((v-1), (v-k), k, (k-\lambda), \lambda)$ -设计。

证明: 显然 $X_1 \setminus X_i, X_2 \setminus X_i, \dots, X_v \setminus X_i$ 所包含的元素属于 $X \setminus X_i$, 而集合 $X \setminus X_i$ 中的每一元素仍然存在于 k 组中, $X \setminus X_i$ 中每一对元素仍然同时出现 λ 次。由于对称的 (v, k, λ) -设计的任意两组都正好有 λ 个共同的元素, 故 $X_1, X_2, \dots, X_{i-1}, X_{i+1}, \dots, X_v$ 中每一区组与 X_i 有 λ 个元素相同。故 $X_1 \setminus X_i, X_2 \setminus X_i, \dots, X_{i-1} \setminus X_i, X_{i+1} \setminus X_i, \dots, X_v \setminus X_i$ 含有 $k-\lambda$ 个元素, 即 $X_1 \setminus X_i, X_2 \setminus X_i, \dots, X_{i-1} \setminus X_i, X_{i+1} \setminus X_i, \dots, X_v \setminus X_i$ 组成 $((v-1), (v-k), k, (k-\lambda), \lambda)$ -设计。证完。

定理：如果 $X_i (i = 1, \dots, v)$ 是关于集合 $X = \{x_1, \dots, x_v\}$ 的对称的 (v, k, λ) -组态，则对于其中任一 X_i ，下列 $v-1$ 个区组： $X_1 \cap X_i, X_2 \cap X_i, \dots, X_{i-1} \cap X_i, X_{i+1} \cap X_i, \dots, X_v \cap X_i$ 构成一个关于集合 X_i 的 $((v-1), k, (k-1), \lambda, (\lambda-1))$ -设计。

证明：显然 $X_1 \cap X_i, X_2 \cap X_i, \dots, X_{i-1} \cap X_i, X_{i+1} \cap X_i, \dots, X_v \cap X_i$ 包含有子集 X_i 中的元素，而且， X_i 中的元素只出现在其中的 $k-1$ 组中， X_i 中任意一对元素在这 $v-1$ 组中同时出现 $\lambda-1$ 次，同时， $X_1 \cap X_i, X_2 \cap X_i, \dots, X_v \cap X_i$ 都包含有 λ 个元素，故 $X_1 \cap X_i, X_2 \cap X_i, \dots, X_{i-1} \cap X_i, X_{i+1} \cap X_i, \dots, X_v \cap X_i$ 构成关于集合 X_i 的 $((v-1), k, (k-1), \lambda, (\lambda-1))$ -设计。证完。

上面两个定理的应用范围须满足 BIBD 的定义，自然也就满足了 (4.10), (6.1), (6.2) 等的要求。据 (6.2) $bk = vr$ ，前一个定理当有

$$(v-1)(k-\lambda) = (v-k)k$$

$$\text{即} \quad v-1 = k(k-1)/\lambda \quad (7.2)$$

对于从已知的六个有限射影平面所构成的对称 (v, k, λ) -设计而言， $v-1 = n^2 + n$ ， $k(k-1)/\lambda = n^2 + n$ ，故 (7.2) 式显然成立。由此我们可以得到 $(6, 4, 3, 2, 1)$ -, $(12, 9, 4, 3, 1)$ -, $(20, 16, 5, 4, 1)$ -， $(30, 25, 6, 5, 1)$ -, $(56, 49, 8, 7, 1)$ -和 $(72, 64, 9, 8,$

1)-共六个新的 BIBD, 其中最简单的是由 $X = \{1, 2, 3, 4\}$ 的元构成的 $\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}$ 。当然, 这个结果是很平凡的。

同样, 据 (6.2), 后一个定理当有:

$$(v-1)\lambda = k(k-1) \quad (7.2)$$

经上面的讨论已知 (v, k, λ) -设计可满足 (7.2), 但是, 所推出的新 BIBD 里出现了 $\lambda = 0$ 的退化现象; 换言之, 这个定理可用的必要条件, 是对称的 (v, k, λ) -设计中 $\lambda > 1$ 。

例: 今有集合 $X = \{1, 2, \dots, 15\}$ 构成对称的 $(15, 7, 3)$ -设计, 求 $(14, 7, 6, 3, 2)$ -设计。

$\{1, 2, 3, 4, 5, 6, 7\},$

$\{1, 2, 3, 8, 9, 10, 11\},$

$\{1, 2, 3, 12, 13, 14, 15\},$

$\{1, 4, 5, 8, 9, 12, 13\},$

$\{1, 4, 5, 10, 11, 14, 15\},$

$\{1, 6, 7, 8, 9, 14, 15\},$

$\{1, 6, 7, 10, 11, 12, 13\},$

$\{2, 4, 6, 8, 10, 12, 14\},$

$\{2, 4, 7, 8, 11, 13, 15\},$

$\{2, 5, 6, 9, 11, 12, 15\},$

$\{2, 5, 7, 9, 10, 13, 14\},$

$\{3, 4, 6, 9, 11, 13, 14\},$

$\{3, 4, 7, 9, 10, 12, 15\},$

$\{3, 5, 6, 8, 10, 13, 15\},$

$\{3, 5, 7, 8, 11, 12, 14\}$

表13. $(15, 15, 7, 7, 3)$ -设计

表13中15个7元组记作 X_i ($i = 1, 2, \dots, 15$), 易于计算当 $i \neq 1$ 时, $X_i \cap X_1$ 的14个3元组为:

$\{1, 2, 3\}, \{1, 2, 3\}, \{1, 4, 5\}, \{1, 4, 5\},$

$\{1, 6, 7\}, \{1, 6, 7\}, \{2, 4, 6\}, \{2, 4, 7\},$

$\{2, 5, 6\}, \{2, 5, 7\}, \{3, 4, 6\}, \{3, 4, 7\},$

$\{3, 5, 6\}, \{3, 5, 7\}.$

表14. $(14, 7, 6, 3, 2)$ -设计

如果应用关联矩阵, 记表13设计的 $(0, 1)$ -矩阵为 A (这里从略), 所求表 14 设计的矩阵为 B , 那么上述求交集的方法就相当于从 A 中去掉 X_1 所在的第一行, 以及去掉 X_1 行元素为0的所有列, 便得到 $X_1 = \{1, 2, \dots, 7\}$ 的一个 BIBD, 其矩阵即 B 。

上述方法都是从一个较大的结构转求一个较小的, 派生的能力不强; 而

$$B = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

递归法提供一种从给定的较小的结构派生出一个较大的来，其意义就不相同了。

定理：如果存在一个 v 阶斯坦纳三连系和一个 w 阶斯坦纳三连系，则必存在一个 vw 阶斯坦纳三连系。

证明：设 $X = \{x_1, \dots, x_v\}$, \mathcal{B}_1 是一个用 X 的元构成的 $S(v)$; $Y = \{y_1, \dots, y_w\}$, \mathcal{B}_2 是一个用 Y 的元构成的 $S(w)$ 。令 $Z = \{z_{ij} : 1 \leq i \leq v, 1 \leq j \leq w\}$ 是 vw 个元素的集合。将 Z 的元排成一个 $v \times w$ 阵列，其中每行对应于 X 的一元，每列对应于 Y 的一元：

$$\begin{array}{c} x_1 \\ x_2 \\ \vdots \\ x_v \end{array} \begin{pmatrix} y_1 & y_2 & \cdots & y_w \\ z_{11} & z_{12} & \cdots & z_{1w} \\ z_{21} & z_{22} & \cdots & z_{2w} \\ \vdots & \vdots & & \vdots \\ z_{v1} & z_{v2} & \cdots & z_{vw} \end{pmatrix} \quad (7.3)$$

现在可以利用 Z 的元素定义一个三连系 \mathcal{B} 了。设 $\{z_{ir}, z_{js}, z_{kt}\}$ 是 Z 的元素的一个三元组，那么它是 \mathcal{B} 中一个三元组当且仅当下列条件之一成立：

(a) $r = s = t$ ，而且 $\{x_i, x_j, x_k\}$ 是 \mathcal{B}_1 中的一个三元组。这等价于元素 z_{ir}, z_{js} 和 z_{kt} 处于 (7.3) 阵列的同一列中，它们所在的那些行对应于 \mathcal{B}_1 中的一个三元组。

(b) $i = j = k$ ，而且 $\{y_r, y_s, y_t\}$ 是 \mathcal{B}_2 中

的一个三元组。这等价于元素 z_{jr} , z_{js} 和 z_{ki} 处于 (7.3) 阵列的同一行中, 它们所在的那些列对应于 \mathcal{B}_2 中的一个三元组。

(c) i, j, k 两两不等, 并且 $\{x_i, x_j, x_k\}$ 是 \mathcal{B}_1 中的一个三元组。同样, r, s, t 两两不等, 并且 $\{y_r, y_s, y_t\}$ 是 \mathcal{B}_2 中的一个三元组。这等价于 (7.3) 阵列的元素 z_{ir}, z_{js}, z_{kt} 处于三个不同的行和三个不同的列中, 这些行与 \mathcal{B}_1 中的一个三元组对应, 这些列与 \mathcal{B}_2 中的一个三元组对应。

观察 (7.3) 阵列里 \mathcal{B} 的任一三元组都没有恰占据两行或两列的现象。设 $\{z_{ir}, z_{js}\}$ 是一个 Z 的元素对, $ir \neq js$, 则有三种情况:

情况 1: $r = s$, 由此 $i \neq j$, 因 \mathcal{B}_1 是 $S(v)$, 则 \mathcal{B}_1 中存在唯一的包含元素对 $\{x_i, x_j\}$ 的三元组 $\{x_i, x_j, x_k\}$, 因而 $\{z_{ir}, z_{jr}, z_{kr}\}$ 是 \mathcal{B} 中包含元素对 $\{z_{ir}, z_{jr}\}$ 的唯一三元组。

情况 2: $i = j$, 由此 $r \neq s$, 因 \mathcal{B}_2 是 $S(w)$, 则 \mathcal{B}_2 中存在唯一的包含元素对 $\{y_r, y_s\}$ 的三元组 $\{y_r, y_s, y_t\}$, 因而 $\{z_{ir}, z_{is}, z_{it}\}$ 是 \mathcal{B} 中包含元素对 $\{z_{ir}, z_{is}\}$ 的唯一三元组。

情况 3: $i \neq j$ 同时 $r \neq s$ 。因 \mathcal{B}_1 是 $S(v)$, 则 \mathcal{B}_1 中存在包含 $\{x_i, x_j\}$ 的唯一三元组 $\{x_i, x_j, x_k\}$; 因 \mathcal{B}_2 是 $S(w)$, 因 \mathcal{B}_2 中存在包含 $\{y_r, y_s\}$ 的唯一三元组 $\{y_r, y_s, y_t\}$, 所以 $\{z_{ir}, z_{js}, z_{kt}\}$ 是 \mathcal{B} 中包含元素对 $\{z_{ir}, z_{js}\}$ 的唯一的三元

组。

综上, \mathcal{B} 是一个 $v w$ 阶的斯坦纳三连系 $S(vw)$ 。证完。

例: 设 $X = \{x_1, x_2, x_3\}$, \mathcal{B}_1 是仅有一个三元组 $\{x_1, x_2, x_3\}$ 构成的 $S(3)$; $Y = \{y_1, y_2, y_3\}$, \mathcal{B}_2 是仅有一个三元组 $\{y_1, y_2, y_3\}$ 构成的 $S(3)$; 今求 3×3 阶的斯坦纳三连系 \mathcal{B} 。令 $Z = \{z_{ij} : i = 1, 2, 3, j = 1, 2, 3\}$ 是 3×3 个元素的集合, 根据 (7.3) 式, 可以将 Z 的元排成 3×3 阵列如下:

$$\begin{array}{c} y_1 \quad y_2 \quad y_3 \\ \begin{array}{c} x_1 \\ x_2 \\ x_3 \end{array} \begin{pmatrix} z_{11} & z_{12} & z_{13} \\ z_{21} & z_{22} & z_{23} \\ z_{31} & z_{32} & z_{33} \end{pmatrix} \end{array} \quad (7.4)$$

(1) 当 $r = s = t$ 时 $\{z_{ir}, z_{js}, z_{kt}\} \in \mathcal{B}$, 故有 $\{z_{11}, z_{21}, z_{31}\}$, $\{z_{12}, z_{22}, z_{32}\}$, $\{z_{13}, z_{23}, z_{33}\}$ 3 个三元组符合条件, 亦即 (7.4) 纵列的 3 个三元组。

(2) 当 $i = j = k$ 时 $\{z_{ir}, z_{js}, z_{kt}\} \in \mathcal{B}$, 故有 $\{z_{11}, z_{12}, z_{13}\}$, $\{z_{21}, z_{22}, z_{23}\}$, $\{z_{31}, z_{32}, z_{33}\}$ 即 (7.4) 3 横行的 3 个三元组符合条件。

(3) 当 r, s, t 两两不等, i, j, k 两两不等时 $\{z_{ir}, z_{js}, z_{kt}\} \in \mathcal{B}$, 故有 $\{z_{11}, z_{22}, z_{33}\}$, $\{z_{12}, z_{23}, z_{31}\}$, $\{z_{13}, z_{21}, z_{32}\}$, $\{z_{11}, z_{23}, z_{32}\}$, $\{z_{12}, z_{21}, z_{33}\}$, $\{z_{13}, z_{22}, z_{31}\}$ 共 6 个三元组符合条件。

综上, 所得到的 3×3 阶斯坦纳三元系 $S(9)$ 就是 $(12, 9, 4, 3, 1)$ -设计; 将 (7.4) 中三行各元顺序写成 $1, 2, \dots, 9$ 就得到第三节表 3, 它是 9 名女学生 4 天内散步的分组方案。

例: 设 $X = \{x_1, x_2, x_3\}$, \mathcal{B}_1 是仅有一个三元组 $\{x_1, x_2, x_3\}$ 构成的 $S(3)$; $Y = \{y_1, \dots, y_7\}$, \mathcal{B}_2 是一个用 Y 的元构成的 $S(7)$ 。今求 3×7 阶的斯坦纳三连系 \mathcal{B} 。令 $Z = \{z_{ij}; 1 \leq i \leq 3, 1 \leq j \leq 7\}$ 是 3×7 个元素的集合。根据 (7.3) 式, 可以将 Z 的元排成 3×7 阵列如下:

$$\begin{array}{c} y_1 \quad y_2 \quad y_3 \quad y_4 \quad y_5 \quad y_6 \quad y_7 \\ \begin{array}{c} x_1 \\ x_2 \\ x_3 \end{array} \left(\begin{array}{cccccc} z_{11} & z_{12} & z_{13} & z_{14} & z_{15} & z_{16} & z_{17} \\ z_{21} & z_{22} & z_{23} & z_{24} & z_{25} & z_{26} & z_{27} \\ z_{31} & z_{32} & z_{33} & z_{34} & z_{35} & z_{36} & z_{37} \end{array} \right) \end{array} \quad (7.5)$$

(1) 当 $r = s = t$ 时 $\{z_{ir}, z_{js}, z_{kt}\} \in \mathcal{B}$, 故有 $\{z_{11}, z_{21}, z_{31}\}, \{z_{12}, z_{22}, z_{32}\}, \dots, \{z_{17}, z_{27}, z_{37}\}$ 共 7 个三元组符合条件, 亦即 (7.5) 纵列的 7 个三元组。

(2) 当 $i = j = k$ 时 $\{z_{ir}, z_{js}, z_{kt}\} \in \mathcal{B}$, 故对 (7.5) 第 1 列的 7 个元有 $\{z_{11}, z_{12}, z_{13}\}, \{z_{11}, z_{14}, z_{15}\}, \{z_{11}, z_{16}, z_{17}\}, \{z_{12}, z_{14}, z_{16}\}, \{z_{12}, z_{15}, z_{17}\}, \{z_{13}, z_{14}, z_{17}\}, \{z_{13}, z_{15}, z_{16}\}$ 共 7 个三元组符合条件, 显见每个三元组的 r, s, t 满足 $\{y_r, y_s, y_t\} \in \mathcal{B}_2$, 亦即足标的第二个数是按照表 6 排出的。同理, 对 (7.5) 第 2 列、第 3 列的 14 个元共有 14 个类似的三元组符合条

件。

(3) 当 r, s, t 两两不等, i, j, k 两两不等时, $\{z_{ir}, z_{js}, z_{kt}\} \in \mathcal{B}$, 故有 $\{z_{11}, z_{22}, z_{33}\}, \{z_{21}, z_{34}, z_{15}\}, \{z_{31}, z_{18}, z_{27}\}, \{z_{12}, z_{24}, z_{36}\}, \{z_{32}, z_{25}, z_{17}\}, \{z_{23}, z_{14}, z_{37}\}, \{z_{13}, z_{35}, z_{26}\}$ 为一类 (7 个) 三元组符合条件。这样的类共可写出不同的 6 个来。这是由于在条件 (c) 下, 对满足 $\{y_r, y_s, y_t\} \in \mathcal{B}_2$ 的 7 个三元组中任一组确定的 r, s, t , 将 1, 2, 3 分配在 $\{z_{ir}, z_{js}, z_{kt}\}$ 里 i, j, k 这三个位置, 不同排列方法的总数是 $3! = 6$ 。于是在条件 (c) 下, 满足 $\{z_{ir}, z_{js}, z_{kt}\} \in \mathcal{B}$ 的三元组的总数是 $7 \times 6 = 42$ 个。

综上, 所得到的 3×7 阶斯坦纳三连系即是 $(70, 21, 10, 3, 1)$ -设计。

从现代设计的观点来看, $S(21)$ 是一个很小的结构, 但如果要我们写出这 70 个三元组, 那确实令人不胜其繁。将 (7.5) 中三行各元顺序写成 1, 2, ..., 21, 再依法编组, 可使问题略为简化。

这个例子可以看作是科克曼著名的 15 名女生问题的推广: 一位教师每天组织她班上的 21 名女生散步。散步时女生排成 7 行, 每行 3 人, 使每个女生有两个同伴。问能否连续组织 10 次散步, 使每 2 名女生至多只有一次排在同一行? 有兴趣的读者, 不妨编写出这个 $S(21)$, 并列出的关

联矩阵。

递归法从一个较小的区组来构造设计，是更为重要的方法，如果追溯这一方法的起源，穆尔在1893年的一篇文章^[44]可能是最早的记录。1961年，哈纳尼给出两个递归定理^[45]，是区组设计理论的重大成果，在霍尔的书《组合论》^[45]中冠以哈纳尼的名字，列为基本定理。上文已提到，他还证明了 $k=3$ 和4时 (b, v, r, k, λ) -设计存在的必要条件也是充分的，为世所瞩目。

以下引用陆家羲使用的对称差集合法来构造一个 BIBD，具有本书引言中所说的纪念性的意义。陆家羲是我国著名的组合数学家，他在令人难以想象的艰苦条件下，独立创造了一套数学方法，在区组设计的领域内，树立了新的里程碑，获得国内外组合数学界的公认和高度评价。这里引用他的手稿（1965）的一部分，反映了当时这个领域的先进水平。当然，对这本小册子而言，陆的文章超出了专题普及读物的水平；但本书作者相信，一定会有研究者对这篇论文的原貌产生兴趣。在长期等待《陆家羲论文集》出版没有新的信息的情况下，作为下文还要谈到的、为陆家羲争取解决科克曼女生问题的优先权努力的一部分，在征得有关方面的同意之后，认为在这样一本专题介绍“科克曼女生问题”的书中引用陆家羲对这个问题的杰出成果是适当的。当然，无庸

讳言，笔者对这样一篇几经改写、多次投稿的论文在从1961年迄今的27年里未能正式发表表示遗憾，它应当尽早和读者见面；同时，作为一个数学史工作者，笔者认为按照解决科克曼女生问题历史进程的原来面貌所作的记录具有更重要的研究价值。

对陆文中各种记号的解释，请阅读“附录”中的第（一）、（二）部分；读者也可以跳过这些内容，直接阅读下面的第八节。

（三）构造B的差集合方法^①

§8. 设 $\tau = \tau'(q) \cup \sigma(m)M(n)$ (3)

其中 M 是阶为 n 的模，把 σM 中的元素 $(y, y', z - z')$ 叫做元素 ξ 和 ξ' 的对称差。如果 $\xi = (y, z)$, $\xi' = (y', z')$ (y 和 $y' \in \sigma$, z 和 $z' \in M$)，从每一对相遇的 ξ 和 ξ' 写出一个对称差 (ξ 和 $\xi' \in \sigma M$)，由 τ 中元素构成的一个区组 b 可以写出 $n(n-1)$ 个对称差 (设 n 是 b 中属于 σM 的元素数)，将这些对称差以任意的次序组成一区组，叫做 b 的对称差组。若 S 是由 τ 中元素构成的设计，则由 S 中每个区组所作出的对称差组的全体叫做 S 的差设计，用 $D_M S$ 来表示。

① 这里引用陆家羲手稿：“平衡不完全区组与可分解不完全区组的构造方法” (1965年3月14日) 中第（三）部分，该文其余部分见本书附录和第九节。

我们用记号 $FY_q[k, \lambda, m, n]$ (或 FY) 来表示 τ 中元素构成的具有以下性质的区组设计:

- (i) 每个区组的大小等于给定的常数 k ;
- (ii) 若 ξ 和 $\xi' \in \tau'$, 则 $A_{FY}(\xi, \xi') = 0$;
- (iii) 若 $\xi \in \tau'$, $y \in \sigma$, 则 $A_{FY}(\xi, P_{\sigma M}^\sigma(y))$ 等于给定的常数 λ ;
- (iv) 设 $(y, y', z) \in \sigma\sigma M$ (y 和 $y' \in \sigma$, $z \in M$), 若 $z=0$ 和 $y=y'$, 则 (y, y', z) 在 $D_M FY$ 中的重复数为 0。在其他情形它在 $D_M FY$ 中的重复数等于 λ 。

如果存在阶为 n 的模 M , 使 $FY_q[k, \lambda, m, n]$ 可以构造, 这事实我们用 $n \in FY_q(k, \lambda, m)$ 来表示。

§9. 下面这命题是显然的。

【命题】若区组集 S, S' 和 $FY_q[k, \lambda, m, n]$ 满足以下的条件 ($S \subset FY_q$), 以 S' 取代 FY_q 中的 S 即得 $FY'_{q+q'}[k, \lambda, m, n]$: ①

(i) FY_q 中的元素属于 $\tau'(q) \cup \sigma(m)M(n)$, S' 中的元素属于 $\tau''(q') \cup \sigma(m)M(n)$, τ'' 与 τ' 互不相交;

(ii) S 不含 τ' 的元素, 且任一 $\sigma\sigma M$ 中的元素在 $D_M S$ 中的重复数等于在 $D_M S'$ 中的重复

① 在处理多个同一种类的设计时, 使用加撇或其他记号来区别, 如此处的 $FY_{q+q'}$ 。——陆家羲注。

数;

(iii) §8的性质 (i) (ii) (iii) 在将 τ' 改为 τ'' , FY 改为 S' 后对 S' 完全适用。

§10. 给出正整数 R 的一个分解式:

$$R = \prod_{i \in E(S)} p_i^{\alpha_i} \quad (4)$$

(p_i 是素数, α_i 是正整数), 取各个有限域 $GF_i(p_i^{\alpha_i})$ 作出它们的直接积, 可以确定一个阶为 R 的可换环 K , 即

$$K = \prod_{i \in E(S)} GF_i(p_i^{\alpha_i}),$$

对任意的 w 和 $w' \in K$, $i \in E(S)$,

$$P_{GF_i}^K(w + w') = P_{GF_i}^K(w) + P_{GF_i}^K(w'),$$

$$P_{GF_i}^K(ww') = P_{GF_i}^K(w)P_{GF_i}^K(w').$$

K 的元素可以用下面的方法分成互不相交的 2^s 个乘法群: 如对任意的 $i \in E(S)$, $P_{GF_i}^K(w) = 0 \iff P_{GF_i}^K(w') = 0$, 则 w 和 w' 属于同一具有某个足码 j 的群 $G_j (j \in E(2^s))$ 。元素 $0 (P_{GF_i}^K(0) = 0, i \in E(S))$ 本身成一群, 记为 G_s , G_j 内的乘法单位元素记作 e_j 。

设在每个 $G_j (j \in E(2^s - 1))$ 内给出一个子群 H_j 。我们考虑 (3) 式中的 $\tau'(q)$ 是空集合, 而 M 是 K 和一个模的直积的情形, 即设:

$$\tau = \sigma(m)M(n)K(R). \quad (5)$$

以下面的性质定义 τ 中元素构成的设计 $FE[k, \lambda, m, n, R]$ (简称 FE);

(i) 每个区组的大小等于给定的常数 k ;

(ii) $FE = \bigcup_{j \in E(2^s - 1)} FS_j$, 对任意的 (x, y, z)

$\in \sigma\sigma M$ 和 $j \in E(2^s - 1)$, 存在一元素 $a \in G_j$, 使得: 当 $w \in aH_j$ 时, (x, y, z, w) 在 $D_{MK}FS_j$ 中的重复数为 λ , 当 $w \notin aH_j$ 时, (x, y, z, w) 在 $D_{MK}FS_j$ 中的重复数为 0 (aH_j 是 H_j 在 G_j 内的一个陪集)。

若存在阶为 n 的模 M 和阶为 R 的环 K (及其子群 H_j), 使 $FE[k, \lambda, m, n, R]$ 可以构造, 这事实我们用 $(n, R) \in FE(k, \lambda, m)$ 来表示。

§11. 【命题】($FE[k, \lambda, m, n, R]$, $T[k, m']$) 是 $FE'[k, \lambda, mm', n, R]$ 。

证明: 设 FE 的元素属于 $\sigma(m)M(n)K(R)$, $T[k, m']$ 的元素属于 $\sigma'(m')$ 。据 §7, (FE, T) 的元素属于 $\sigma\sigma' M K$ ①。令 $FS'_j = (FS_j, T)$, 则 $(FE, T) = (\bigcup_{j \in E(2^s - 1)} FS_j, T) = \bigcup_{j \in E(2^s - 1)} (FS_j, T) = \bigcup_{j \in E(2^s - 1)} FS'_j$ 。取 $FE' = (FE, T)$, 需要证明的是, §10 的性质 (i) 和 (ii) 在将 σ 改为 $\sigma\sigma'$ 、 FE 和 FS_j 分别改为 FE' 和 FS'_j 后在此完全成立。

任意取 $b \subset FS_j$, $j \in E(2^s - 1)$ 。由定义 (§6) 可令 b 中第 a 个元素与 (b, T) 中每组的第 a 个

① 据 §7 (EF, T) 的元素属于 $\sigma MK \sigma'$, 改写成 $\sigma\sigma' MK$ 于实质并无影响。——陆家羲注。

元素相对应 ($a \in E(k)$)。这样, b 中两个元素 (x, z, w) 和 (x', z', w') 的对称差 $(x, x', z - z', w - w')$ 对应于 (b, T) 中元素的下面一系列对称差 (x 和 $x' \in \sigma$, z 和 $z' \in M$, w 和 $w' \in K$),

$$\begin{aligned} & ((x, y_1), (x', y'_1), z - z', w - w'), \\ & ((x, y_2), (x', y'_2), z - z', w - w'), \\ & \dots\dots\dots \end{aligned}$$

$$((x, y_{m'2}), (x', y'_{m'2}), z - z', w - w'),$$

而 $(y_1, y'_1), (y_2, y'_2), \dots, (y_{m'2}, y'_{m'2})$ 是 $\sigma'\sigma'$ 的全体元素 (§4)。由此可知, $(\sigma\sigma')(\sigma\sigma')MK$ 中的元素 $((x, y), (x', y'), z, w)$ 在 $D_{MK}FS_j$ 中的重复数不依赖于 y 和 y' 而等于 (x, x', z, w) 在 $D_{MK}FS_j$ 中的重复数。于是, 从 §10 的性质 (ii) 对 FE 成立推知对 FE' 也成立。性质 (i) 的成立则属显然。

【系】若 $(n, R) \in FE(k, \lambda, m)$, $m' \in \tau(k)$, 则 $(n, R) \in FE(k, \lambda, mm')$ 。

§12. 设 $\tau = \tau'(q) \cup \sigma(m)M(n)\sigma'(m')$ 。给定 $z \in M$, 定义从 τ 到 τ 上的单调映象 φ_z :

$$\text{当 } \xi \in \tau', \varphi_z(\xi) = \xi;$$

$$\text{当 } \xi \in \sigma M \sigma', P_{\sigma M \sigma'}^{\sigma M \sigma'}(\varphi_z(\xi)) = P_{\sigma M \sigma'}^{\sigma M \sigma'}(\xi)$$

$$P_M^{\sigma M \sigma'}(\varphi_z(\xi)) = P_M^{\sigma M \sigma'}(\xi) + z,$$

$$P_{\sigma'}^{\sigma M \sigma'}(\varphi_z(\xi)) = P_{\sigma'}^{\sigma M \sigma'}(\xi)。$$

φ_z 可以推广到 τ 中元素构成的区组集 S 。如果 b 是 τ 中元素构成的区组, 于是 $\varphi_z(b)$ 是将 b 中

每个元素 ξ 改成 $\varphi_z(\xi)$ 而得的区组。将 S 中的每个区组 b 改成 $\varphi_z(b)$ 而得的区组集就记作 $\varphi_z(S)$ 。

定义 $\Phi_M(S) = \bigcup_{z \in M} \varphi_z(S)$ 。

考虑 $m' = 1$, 即 σ' 可略去的情形。我们证明下面的命题成立。

【命题】

(i) 若 ξ 和 $\xi' \in \tau'$, 则 $\Lambda_{\Phi_M S}(\xi, \xi') = \Lambda_S(\xi, \xi')$;

(ii) 若 $\xi \in \tau'$, $\xi' \in \sigma M$, 则 $\Lambda_{\Phi_M S}(\xi, \xi') = \Lambda_S(\xi, P_{\sigma M}^{\sigma M} P_{\sigma M}^{\sigma M}(\xi'))$;

(iii) 若 ξ 和 $\xi' \in \sigma M$, 则 $\Lambda_{\Phi_M S}(\xi, \xi')$ 等于 ξ 和 ξ' 的对称差在 $D_M S$ 中的重复数。

证明: (i)显然, 设 $\xi \in \tau'$, $\xi' \in \sigma M$, ξ 与 ξ' 在 S 的某个组 b 以序 (α, β) 相遇。如果 $\xi'' \in P_{\sigma M}^{\sigma M} P_{\sigma M}^{\sigma M}(\xi')$, 则存在唯一的 $Z = P_{\sigma M}^{\sigma M}(\xi') - P_{\sigma M}^{\sigma M}(\xi'')$, 使 ξ 和 ξ' 在 $\varphi_z(b)$ 中以序 (α, β) 相遇。如果 $\xi'' \in P_{\sigma M}^{\sigma M} P_{\sigma M}^{\sigma M}(\xi')$, 则不存在 z 使 ξ 和 ξ' 在 $\varphi_z(b)$ 中以序 (α, β) 相遇。由此见(ii)成立。对于(iii), 若 ξ 和 ξ' 的对称差在 $D_M b (b \subset S)$ 中所出现的一次相应于 ξ'' 和 ξ''' 在 b 中以序 (α, β) 相遇, 则存在唯一的 $Z = P_{\sigma M}^{\sigma M}(\xi) - P_{\sigma M}^{\sigma M}(\xi'')$ 使 ξ 和 ξ' 在 $\varphi_z(b)$ 中以序 (α, β) 相遇。而如果 ξ'' 和 ξ''' 的对称差不等于 ξ 和 ξ' 的对称差, 则前者以序 (α, β) 在 b 中相遇蕴涵着不存在 Z 使 ξ 和 ξ' 在 $\varphi_z(b)$ 中以同样的序 (α, β) 相遇。由此见(iii)成立。

§ 13 考虑形如(5)式的集合: $\tau = \sigma(m)$

$M(n)K(R)$ 。给出 τ 中元素构成的一个区组集 S 和 K 中的一个元素 a 后,用 a 去乘 S 中各元素在 K 上的投影而得的区组集记作 $\langle S, a \rangle$ 。若元素集 $A \subset K$, 定义 $\langle S, A \rangle = \bigcup_{a \in A} \langle S, a \rangle$ 。以后需要

从 H_j 在 G_j 内的每一陪集中任意选出一个元素组成元素集 A_j , A_j 所含的元素数显然等于 H_j 在 G_j 中的指数。

【定理】 设 $FE \subseteq [k, \lambda, m, n, R]$ 中的元素属于 $\sigma(m)M(n)K(R)$, $B_q \subseteq [k, \lambda, mn+q]$ 的元素属于 $\tau'(q) \cup \sigma MG_2^s$, B_q 包含 τ' 中元素构成的 $B' \subseteq [k, \lambda, q]$, 则

$\Phi_M(\bigcup_{j \in E(2^{m-1})} \langle FS_j, A_j \rangle) \cup B_q$ 是 $FY_q \subseteq [k, \lambda, mn, R] \cup B'$, 其中 FY_q 的元素属于 $\tau = \tau' \cup \sigma MK$ 。①

证明: 令 S 是 $\Phi_M(\bigcup_{j \in E(2^{m-1})} \langle FS_j, A_j \rangle) \cup B_q$ 除去 B' 后的区组集, 只须证明 S 满足 FY_q 的条件。§8(i)显然成立, τ' 的元素在 S 中只在属于 B 的组内出现。由于 B 中的 B' 已被去掉, 所以§8(ii)也成立。

设 $\xi \in \tau'$, $(y, z) \in \sigma M$ 。集 $P_{\sigma MK}^{\sigma M}((y, z))$ 中仅有一个元素 (在 K 上的投影是0) 与 ξ 在 S 中属于 B 的组内相遇 λ 次, 因此§8(iii)也成

① (3) 式中的 σ 相当于这里的 σM , M 相当于这里的 K 。

立。

现在考虑关于 $D_K S$ 的 §8 (iv) :

1. 设 $\xi \in (\sigma M)(\sigma M)K$, $P_{(\sigma M)(\sigma M)K}^{(\sigma M)(\sigma M)K}(\xi) = 0$. 这时 ξ 只能在 $D_K B$ 内出现, 如果 $P_{(\sigma M)(\sigma M)K}^{(\sigma M)(\sigma M)K}(\xi) = ((y, z), (y, z))$ ($y \in \sigma, z \in M$), 则 ξ 之出现蕴涵 B 的某一组有同一元素的重复, 这是不可能的. 如果 $P_{(\sigma M)(\sigma M)K}^{(\sigma M)(\sigma M)K}(\xi) = ((y, z), (y', z'))$, $(y, z) \neq (y', z')$, 则 ξ 在 $D_K B$ 中的重复数等于 σMK 中的元素 $(y, z, 0)$ 和 $(y', z', 0)$ 在 B 内的相遇数, 因此 ξ 在 $D_K S$ 中的重复数是 λ .

2. 设 $\xi \in (\sigma M)(\sigma M)K$, $P_{(\sigma M)(\sigma M)K}^{(\sigma M)(\sigma M)K}(\xi) \in G_j$, $j \in E(2^s - 1)$. 这时 ξ 只能在 $D_K \Phi_M \langle FS_j, A_j \rangle$ 内出现^①. 写出 ξ 的表达式 $\xi = ((y, z), (y', z'), w)$ (y 和 $y' \in \sigma, z$ 和 $z' \in M, w \in K$), 其在 $D_K \varphi_{z''}(b)$ 内出现的条件首先是 $(y, y', z - z', w)$ 在 $D_{MK} b$ 内出现 ($z'' \in M, b \subset \langle FS_j, A_j \rangle$). 而若 $(y, y', z - z', w)$ 在 $D_{MK} b$ 内出现的一次相应于 ξ' 和 ξ'' 在 b 内以序 (α, β) 相遇, 则存在唯一的 z'' , 使 ξ 在 $D_K \varphi_{z''}(b)$ 内出现, 并且相应于 $\varphi_{z''}(\xi')$ 和 $\varphi_{z''}(\xi'')$ 在 $\varphi_{z''}(b)$ 内以序 (α, β) 相遇. 由此知 ξ 在 $D_K \Phi \langle FS_j, A_j \rangle$ 内的重复数等于 $(y, y', z - z', w)$ 在 D_{MK}

① 易知 $\Phi_M(\bigcup_{j \in E(2^s - 1)} \langle FS_j, A_j \rangle) = \bigcup_{j \in E(2^s - 1)} \Phi(\langle FS_j, A_j \rangle)$.

$\langle FS_i, A_i \rangle$ 内的重复数。后者据 § 10 (ii) 及 A_i 的定义等于 λ ，因此 § 8(iv) 也成立。定理证毕。

【系】 若 $(n, R) \in FE(k, \lambda, m)$, $q + mn \in B_q(k, \lambda)$, 则 $R \in FY_q(k, \lambda, mn)$ 。

§ 14. **【定理】** 若 $n \in FY_q(k, \lambda, m)$, $q \in B(k, \lambda)$, 则 $q + mn \in B_q(k, \lambda)$ 。

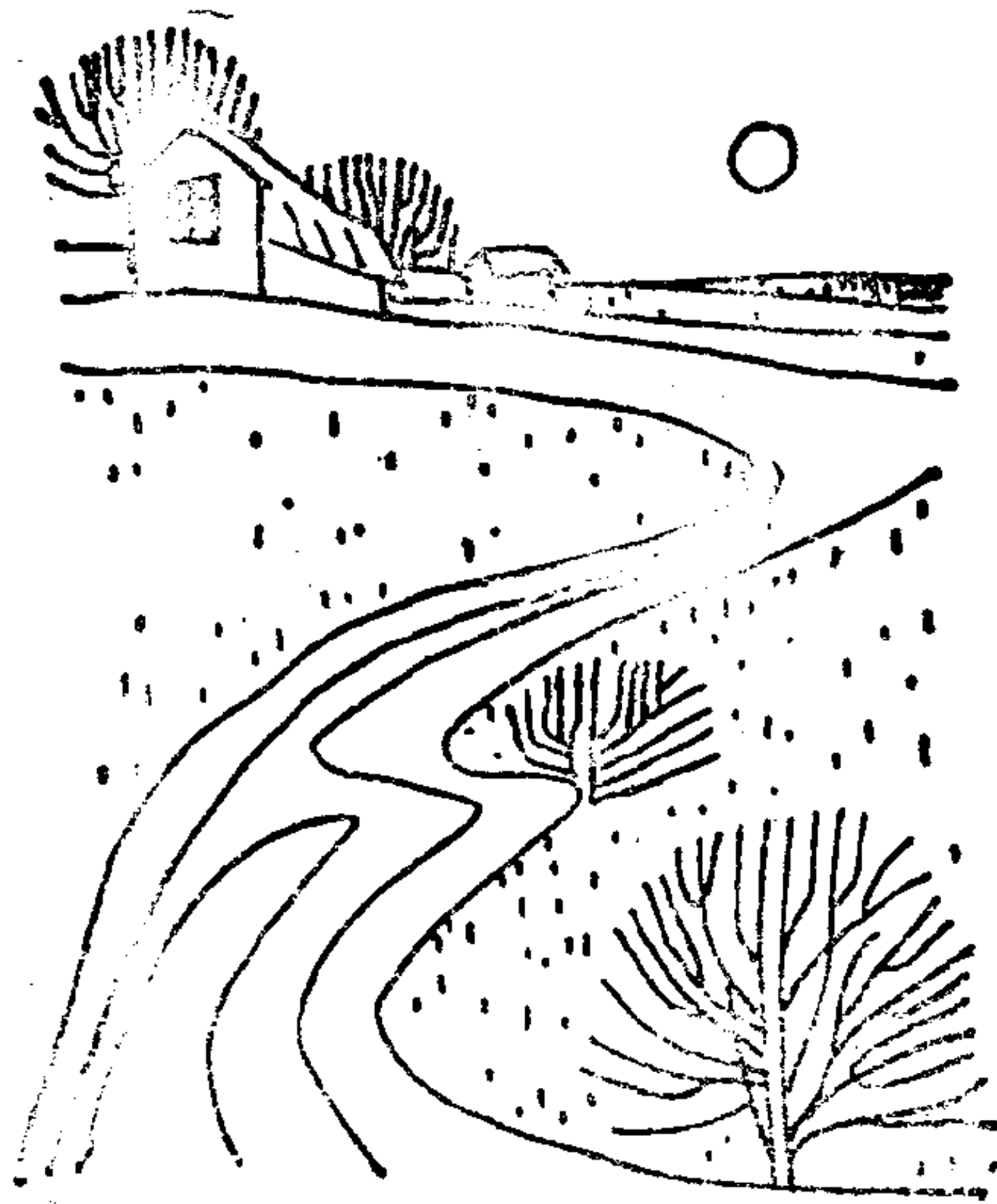
证明：令 $\tau = \tau'(q) \cup \sigma(m)M(n)$ ，取 τ 中元素构成的 $FY_q[k, \lambda, m, n]$ 和 τ' 中元素构成的 $B'[k, \lambda, q]$ 。命 $S = \Phi_M(FY_q[k, \lambda, m, n]) \cup B'[k, \lambda, q]$ ，我们证明 S 即是 $B_q[k, \lambda, q + mn]$ 。

§ 1 (i) 和 (ii) 对 S 显然成立。若 ξ 和 $\xi' \in \tau'$ ，据 § 8(ii) 和 § 12(i)，他们不在 $\Phi_M(FY_q)$ 内相遇，但在 B' 内相遇 λ 次。在 $\xi \in \tau'$, $\xi' \in \sigma M$ 的情形，§ 1(iii) 的成立可由 § 12(ii) 和 § 8(iii) 得到证明， ξ 和 $\xi' \in \sigma M$ 的情形则从 § 12(iii) 和 § 8(iv) 可见。定理于此证毕。

【系】 若 $(n, R) \in FE(k, \lambda, m)$, $q + mn \in B_q(k, \lambda)$, 则 $q + mnR \in B_q(k, \lambda)$ 。

证明：从 $q + mn \in B_q(k, \lambda) \implies q \in B(k, \lambda)$ ，再应用 § 13 系及上面的定理即得证明。

八、科克曼系和科克曼 三连系



对于一般的 (v, k, λ) -设计, 如果进一步要求它的所有区组可分成若干个“平行类”, 则称这种设计为“可分解的平衡不完全区组设计”, 简称 RBIB, 记作 $RB[k, \lambda; v]$ 。所谓“平行类”, 指这样的区组类, 其中全部区组正好构成集合 X 的一个“分划”。所谓“分划”, 是集合 S 的划分为子集族 $S_i (i = 1, \dots, t)$ 的可分性质, 使得 $\bigcup_{i=1}^t S_i = S$, 且对 $i \neq j$ 有 $S_i \cap S_j = \emptyset$ 得到满足。

具体到斯坦纳三连系, 设 n 是非负整数, 一个阶数 $v = 6n + 3$ 的斯坦纳三连系如果再满足下述附加条件, 就称为一个阶数 $v = 6n + 3$ 的科克曼三连系, 即这个斯坦纳三连系中 $b = (2n + 1)$

$(3n + 1)$ 个三连的集合可以划分成 $3n + 1$ 个平行类, 每类都含有 $2n + 1$ 个三元组, 而且 $v = 6n + 3$ 个元素中的每一个在以上 $3n + 1$ 平行类中正好出现一次。

例如, 当 $n=0$ 时 $v=3$, 这时 $S(3)$ 或 $RB[3, 1; 3]$ 是退化的。

当 $n=1$ 时, $v=9$, 这时的斯坦纳三连系 $S(9)$ 如前表 3 所列, 也是科克曼三连系 $RB[3, 1; 9]$, 它的所有区组可分成 $3n+1=4$ 个平行类, 即安排 4 天的分划。

当 $n=2$ 时, $v=15$, 这时 $S(15)$ 如表 2 所列, 这是科克曼女生问题的原来形式, 它有 7 个平行类, “科克曼” 三连系因此而得名。

我们已经看到, 当 v 的数值稍微增大一些, $RB[3, 1; v]$ 区组数便有巨大的增加, 因此有必要按照平行类改进这些三元组的写法。以 $RB[3, 1; 21]$ 为例, 它由 10 个平行类组成, 每类 7 个区组, 用 $[x]$ 表示 x 的模 7 数值, 即以 7 为模的剩余类。当 $k=0, 1, \dots, 6$ 时, 下面的前三个区组各给出一类; 而后七个区组则对同一个 k 组成一类:

$$\begin{aligned} & \{[k], 14+[1+k], 7+[3+k]\}; \\ & \{7+[k], [1+k], 14+[3+k]\}; \\ & \{14+[k], 7+[1+k], [3+k]\}; \\ & \{[k], [1+k], [3+k]\}; \\ & \{7+[k], 7+[1+k], 7+[3+k]\}; \\ & \{14+[k], 14+[1+k], 14+[3+k]\}; \\ & \{[2+k], 7+[4+k], 14+[5+k]\}; \\ & \{7+[2+k], 14+[4+k], [5+k]\}; \\ & \{14+[2+k], [4+k], 7+[5+k]\}; \end{aligned}$$

$\{[6+k], 7+[6+k], 14+[6+k]\}$ 。

仅举两个平行类为例。第三个区组,当 $k=0, \dots, 6$ 时得到一类:

$\{14, 8, 3\}, \{15, 9, 4\}, \{16, 10, 5\}, \{17, 11, 6\}, \{18, 12, 0\}, \{19, 13, 1\}, \{20, 7, 2\}$ 。

当 $k=6$ 时, 后七个区组给出一类:

$\{6, 0, 2\}, \{13, 7, 9\}, \{20, 14, 16\}, \{1, 10, 18\}, \{8, 17, 4\}, \{15, 3, 11\}, \{5, 12, 19\}$ 。

这样, 可以轻易地写出所有十个平行类来。

关于RBIB的一般概念是由波斯在1942年首先提出的。较广泛的 $RB[k, 1; v]$ 被称为科克曼系。斯坦纳系具备的许多性质也为科克曼系所具有, 但对科克曼系特殊性质的研究并不充分。从历史上看, 第一个大问题是存在性问题。

因为一个平行类是 v 元集 X 的一个分划, 而每个区组均含有 X 的 k 个元素, 故每个平行类应包含 v/k 个区组, 又因区组总数 $b = \frac{\lambda v(v-1)}{k(k-1)}$,

所以平行类的数目应是

$$\frac{b}{v/k} = \frac{\lambda(v-1)}{k-1} \quad (8.1)$$

这就给出了 $RB[k, \lambda; v]$ 存在的必要条件:

$$v \equiv 0 \pmod{k},$$

$$\lambda(v-1) \equiv 0 \pmod{(k-1)} \quad (8.2)$$

同研究BIB的思路一样, 人们也提出了类似

的问题：同余式组(8.2)是否也是 RBIB 存在的充分条件？

当 $k=1$ 和 $k=2$ 时，没有必要讨论；当 $k=3$ ， $\lambda=1$ 时，(8.2)式等价于 $v \equiv 3 \pmod{6}$ ，这就是为什么科克曼三连系的阶数一定是 $6n+3$ 的道理。又由于科克曼三连系一定是斯坦纳三连系，

故它的区组数必满足(6.10) $b = \frac{1}{6}v(v-1) =$

$(6n+3)(6n+2)/6 = (2n+1)(3n+1)$ 。这里 $3n+1$ 是平行类的个数， $2n+1$ 是三元组的个数。但是，阶数为 $6n+3$ 的斯坦纳三连系是否一定构成科克曼三连系的问题却不是一个简单的问题，由于 RBIB “可分解性”所带来的明显的难度，即使对于 $RB[3, 1; v]$ 这一局部性问题，在一百多年的时间里毫无进展。组合数学中，

“科克曼三连系存在的必要条件是否也是充分的”被称为“科克曼女生问题”，本书的书名即由此而来。

60年代初，一位刚走出大学校门的中国大学生陆家羲解决了这一数学史上著名的世界难题。

“陆家羲，1935年生，上海市人。1949年初中毕业，1951年10月应前东北电器工业管理局招聘去沈阳受短期训练。1952年5月—1957年在哈尔滨电机厂工作，科员。1957年—1961年在吉林师范大学物理系学习。1961年—1962年分配在包头钢铁学院工作。1962年—1983年在包头市教育

局所属各单位工作。现职：包头九中物理教员”。^[46]

陆家羲在1961年12月写成题为“寇克满系列和斯坦纳系列的制作方法”的论文，1963年3月经过改写，1965年3月又经改写，取名“平衡不完全区组与可分解平衡不完全区组的构造方法”。这三篇论文因故均未能发表。陆已于1983年10月去世，清理他的文稿时仅发现了投稿及退稿的记录、信件和1965年的那篇论文。1961年和1963年的两篇没有找到，这是令人感到十分遗憾的。

陆家羲说：“一九六一年我解决了一个著名数学难题——寇克满女生问题。”^[46]根据现有的、确凿的材料，在1961—1965年期间，陆确实从事了这方面的研究工作，经我国组合数学工作者、苏州大学吴利生教授等同志审定，1965年的论文是正确的^[47]，即陆家羲确实解决了科克曼女生问题。

接着，1971年，雷·乔得赫里和威尔逊著文“科克曼女生问题的解”^[47]，证明了 $v \equiv 3 \pmod{6}$ 确实是 $RB[3, 1; v]$ 存在的充分条件，此文发表在美国数学会1971年《纯粹数学讨论会会议录》中，得到世界组合数学界的公认。文中对所有 $n = 0, 1, 2, 3, \dots$ 指出了怎样构造 $v = 6n + 3$ 阶科克曼三连系。在布鲁尔迪所著的《组合学导引》中理所当然地引述了这一历史成就。由于此书有相当的普及面，所以今天学习或研究组合数学的人

们，都知道雷·乔得赫里和威尔逊的名字。

在60年代，是否还有人解决过这个世界难题呢？我们注意到，1977年美国出版的《科学技术百科全书》（第4版）第1卷《数学》中“组合论”条目内称^[13]，女生问题在1968年已解决。如果该条目的作者布鲁劳斯基指的不是1971年的成果的话，那么这种说法迄今尚未找出事实依据。

本书作者作为一个数学史工作者，认为陆家羲至迟在1965年已独立解决了科克曼女生问题，较之现今公认的成果至少早六年。在科学史上，科学技术成果的首创权的争议并不罕见，在闭塞的时代较多出现，在开放的时代也难以避免。科学对向她提供有价值思想的一切来源都表示了同样的尊重，陆家羲首创性的成果也不应当埋没在历史的尘埃之中。这同样也是理所当然的。的确，他的论文在当时未能发表，对争取承认首创权是不利的条件，但是，对科学史而言，这并非是一个不可挽回的缺憾。

本书将在第九节“陆家羲：科克曼女生问题的解”中把他的“平衡不完全区组与可分解平衡不完全区组的构造方法”关于RBIB的部分介绍给读者，可以使您随着论文的展开而进入当时区组设计的前沿工作，深入体会解决科克曼女生问题的思路和方法；同时作为恢复历史原来面貌的努力的一部分，藉以复制一份珍贵的科学史史

料。书末附以该文关于BIB的构造方法，使该文的全貌与读者见面。

1972年，哈纳尼·雷·乔得赫里和威尔逊合作，证明了(8.2)式是 $RB[4, 1; v]$ 存在的充分条件；1974年，哈纳尼独立证明了：除去 $v=6$ 以外，(8.2)式也是 $RB[3, 2; v]$ 存在的充分条件。

与BIBD设计的情况相似，当 $k \geq 5$ 时，即使限定 $\lambda = 1$ ，也有虽满足(8.2)式但相应的 $RB[k, \lambda; v]$ 却不存在的例子。于是，人们对 RBIB 也提出了类似于 (v, k, λ) -设计的、退一步的猜想。

1973年，雷·乔得赫里和威尔逊首先对 $\lambda = 1$ 的情形给出如下结论：对给定的正整数 k ，除了有限个正整数 v 之外， $RB[k, 1; v]$ 存在的充要条件是(8.2)式成立。^[48]

对一般的 λ 的结论，则是陆家羲在1979年7月获得的，^[49]这篇论文已发表在《数学学报》1984年第4期上，题为“可分解平衡不完全区组设计的存在性理论”。他得到的结论是：对于给定的正整数 k 和 λ ，除了有限个正整数 v 之外， $RB[k, \lambda; v]$ 存在的充要条件是(8.2)式成立。

陆家羲的这一成果在国内外组合数学界获得了高度评价，认为这一结果是整个区组设计理论中带有基本重要性的一个定理，其意义以及对以后工作的影响是绝不会在下面第十一节所要介绍

的大集定理之下的。我国组合数学工作者沈颢在国外向美、加、欧、日等地的组合数学家们介绍了陆家羲的这一成就，他们对此十分感兴趣，评价很高。由于《数学学报》以中文发表，国外学者非常希望能将此文译成英文，一位数学家还打算在他编的《离散数学年鉴》上发表，以扩大其影响。

另外，威尔逊在1975年证明了：对给定的正整数 k ，除了有限对正整数 (v, λ) 之外， $RB[k, \lambda; v]$ 存在的充要条件是 $v \geq k$, $\lambda(v-1) \equiv 0 \pmod{(k-1)}$, $\lambda(v(v-1)) \equiv 0 \pmod{k(k-1)}$ ⁽⁴²⁾。于是，人们自然要猜测，是否有一个更强的结论，与威尔逊 1975 年关于 BIBD 的结论相对应，即：

对给定的正整数 k ，除了有限对正整数 (v, λ) 外， $RB[k, \lambda; v]$ 存在的充要条件是 (8.2) 式成立。

这一问题尚未解决。所以，迄今为止，陆家羲的结果仍是在 RBIB 存在性理论中最好的、也是相当齐整的结果。⁽⁵⁰⁾

虽然在区组设计中有许多问题未能解决，但人类的认识能力却不情愿局限在这些似乎是已知的领域，在继续研究的同时，又不断开辟出新的天地，一个个巨大、复杂的结构呈现在面前或想象之中，一个个新的难题被提出来，它们造成了新的困惑，激发起新的热情，似乎形成了对人类的

耐心和智慧永恒的挑战——而在实质上，这是人类自信心的体现。

我们已经知道，可分解平衡不完全区组设计 RBIB 是平衡不完全区组设计 BIBD 的特例，而 BIBD 又是更广泛的一类 t -(v , k , λ) 设计的特例。 t -(v , k , λ) 设计简称 t -设计，在第二节中只是简单地提到了它。只要将 BIBD 的定义中“2-子集”改为“ t -子集”就得到它的定义。在这个新范畴中，BIBD 应当称做 2-设计。斯坦纳系则一般泛指 t -(v , k , 1) 设计，记作 $S(t, k, v)$ 。于是在此新记法下，斯坦纳三连系和科克曼三连系分别记为 $S(2, 3; v)$ 和 $S_K(2, 3; v)$ ，简记为 $S(v)$ 和 $S_K(v)$ 。

在 BIBD 范围内，除去 RBIB 之外，还有“仿射可分解 BIB” (ARBIB)、“对称 BIBD” (SBIB) 等各种设计；与 BIBD 相对应的，有“完全区组设计”（如拉丁方）、“部分平衡不完全区组设计” (PBIB)，等。

在三连系的研究内容方面，新的概念不断涌现，诸如广义 (extended) 三连系、仿射 (affine) 三连系、准 (almost) 三连系、拟 (nearly) 科克曼三连系、阿贝尔 (Abelian) 斯坦纳三连系、霍尔 (Hall) 三连系、曼德尔逊 (Mendelsohn) 三连系、小 (small) 斯坦纳系等。对斯坦纳系的研究与正交拉丁方、广义罗姆 (Room) 方、有限几何、近世代数、数论、图论、矩阵论、编码、拟

阵、拟群等联系起来，极大地丰富了它的内容，并获得了更加深刻而普遍的结果。

在本书第十二节中，将引入Nim三连系的概念，在第一节中已介绍了它的悠久的历史背景，我们将证明Nim三连系是斯坦纳三连系的一种，并在满足 $v \equiv 0 \pmod{3}$ 的条件下，又是科克曼三连系。

九、陆家羲：科克曼 女生问题的解^①



(四) 构造 RB 的差集合方法

§15. 考虑形如 (3) 式的集合: $\tau = \tau'(q) \cup \sigma(m)M(n)$ 。满足下面条件的 τ 中元素构成的设计记为 $RFY[k, \lambda, m, n]$:

- (i) 它是 $FY_q[k, \lambda, m, n]$,
- (ii) 它的全体区组可以组成下面的两种行:
 甲种行—— τ 的每个元素恰出现一次;
 乙种行—— τ' 的元素不出现, 对任意的 $y \in \sigma$,
 恰包含 $P_{\sigma M}^{\circ}(y)$ 中的一个元素。

如果存在阶为 n 的模 M 使 $RFY_q[k, \lambda, m, n]$ 可以构造, 这事实我们用 $n \in RFY_q(k, \lambda, m)$

① 本节引用陆家羲手稿: “平衡不完全区组与可分解平衡不完全区组的构造方法”(1965年3月14日)中第(四)(五)(六)部分; 该文其余部分见本书附录和第七节。

来表示。

【定理】若 $n \in RFY_q(k, \lambda, m)$, $q \in RB(k, \lambda)$, 则

$$q + mn \in RB_q(k, \lambda).$$

证明: 令 $\tau = \tau'(q) \cup \sigma(m) M(n)$, 取 τ 中元素构成的 $RFY_q[k, \lambda, m, M]$ 和 τ' 中元素构成的 $RB'[k, \lambda, q]$. 令 $S = \Phi_M(RFY_q[k, \lambda, m, n]) \cup RB'[k, \lambda, q]$, 从 §14 知 S 是 $B_q[k, \lambda, q + mn]$.

取 S 中每个形如 $\varphi_z(h_\alpha)$ 的区组集组成一个行 (这里 h_α 是 RFY 的任一甲种行, z 是 M 的任意元素). 这样组成的行显然满足 RB 的行的条件. 又取 S 中每个形如 $\Phi_M(h_\beta) \cup h$ 的区组集组成一个行, 它也满足 RB 的行的条件 (h_β 是 RFY 的任一乙种行, h 是 RB' 的任一行). 由于 RB' 的行的数目等于 RFY_q 中乙种行的数目, 这两种组成行的手续可以取尽 S 的区组, 如果不是这样, 就要推出 τ' 中元素与 σM 中元素在 S 中的重复数不同的矛盾. 因此 S 是 $RB_q[k, \lambda, q + mn]$, 包含 $RB'[k, \lambda, q]$.

§16. 上节的定理对应于 §14 的定理的可分解情况. 而在 $q=0$ 或 1 的特殊情况, §14 的定理化为众所周知的 Bose 定理【5】【6】^①. 应用此定理须先构造 FY , (三) 的其他各节便大都是服务于构造 FY 这个目的而写的, 其中 FE 的提出为

① 参考文献列于本书附录之末。——本书作者注。

的是利用环中的乘法。在限于伽罗华域的情形，利用乘法前人也考虑过，那往往是给出初始区组后用适当的子群去乘^①，而在应用 FE 构造 FY 时是用 A_i 相乘 (§13)。所提供的构造 FY 的方法自然也适用于构造 RFY ，只须注意附加的行的条件。

作为例子，后面 ((六)(七)) 用 (三)(四) 的方法证明构造 $k=3, 4$ 和 $\lambda=1$ 的 RB 的充要条件。在这些讨论中也可以见到寻找适合的子群 H_i 的可能的方法。但我们先在 (五) 陈述两种组合方法，在一定的条件下，为了确定给定参数的 RB 的可构造性，组合方法较之差集方法便于应用。构造 $k=3, \lambda=1$ 的 RB 等价于解少女问题或 Kirkman 问题，前人的工作在【7】内有一总结。据同一文献，对于构造 $k=4, \lambda=1$ 的 RB ，前人研究到 $v < 196$ ^②。

(五) 构造 RB 的组合方法^③

§17. 【定理】若 kq_1 和 $kq_2 \in RB(k, 1)$,

① 如在【6】的表11.1中的若干设计。——陆家羲注。

② 文献【7】作者不久前才见到，该书所据以写作的材料仍未找见。——陆家羲注。

③ 我们只限于 $\lambda=1$ 的 RB (供后面的需要)，但所述方法可推广到一般的 B 设计。用组合方法构造 B 的一个较深入的研究见文献【11】。——陆家羲注。

$q_1 \in RT(k)$, 则

$$kq_1 q_1 \in RB_{kq_1}(k, 1) \textcircled{1}.$$

证明: 1. 命 $\tau = \sigma(kq_1)\sigma'(q_1)$. 取 σ' 的元素构成 $RB'[k, 1, kq_1]$, 并以足码将其中的区组编号成 $b_{\alpha\beta}$, 使得同一行中的区组的前一足码相同 ($\beta \in E(q_1)$, $\alpha \in E(r)$, r 是 RB' 的行的数目). 根据每一组 $b_{\gamma\beta}$ ($\beta \in E(q_1)$), 取元素集 $\{x; x \in \sigma\sigma', P_{\sigma\sigma'}^{\sigma\sigma'}(x) \in b_{\gamma\beta}\}$ 构成 $RB^{(\beta)}[k, 1, kq_1]$, 并将其中的行编号成 $h_{\gamma\beta}$, 后一足码如同 $RB^{(\beta)}$ 左上角的 (β) , 指明所从来的区组 $b_{\gamma\beta}$ ($\gamma \in E(r')$, r' 是 $RB^{(\beta)}$ 的行的总数)。

取 τ 中元素构成的设计 S_1 :

$$S_1 = \bigcup_{\gamma \in E(r')} \left(\bigcup_{\beta \in E(q_1)} h_{\gamma\beta} \right),$$

令其中每个形如 $\bigcup_{\beta \in E(q_1)} h_{\gamma\beta}$ 的区组集组成一个新的行, 这样的行满足 RB 的行的条件。

2. 取 σ' 的元素构成 $RT[k, q_1]$. 根据每一组 $b_{\alpha\beta}$ ($\alpha \in E(r-1)$, $\beta \in E(q_1)$) 构造 $(b_{\alpha\beta}, RT)$, 并将其中的行编号成 $h'_{\delta\alpha\beta}$ ($\delta \in E(q_1)$), 后 β 个足码指明所从来的区组 $b_{\alpha\beta}$. 取 τ 中元素构成的设计 S_2 :

$$S_2 = \bigcup_{\substack{\delta \in E(q_1) \\ \alpha \in E(r-1)}} \left(\bigcup_{\beta \in E(q_1)} h'_{\delta\alpha\beta} \right)$$

① 在 $k=3$ 时就是 Harison 定理。——陆家羲注。

以其中每个形如 $\beta \in E(q_1)$ $\bigcup h'_{s\beta}$ 的区组集组成一个新的行，从 § 7 (iii) 容易看出，这样的行也满足 RB 的行的条件。

3. 令 $S = S_1 \cup S_2$ ，则 S 是 $RB_{kq_2}[k, 1, kq_1 q_2]$ 。它包含 $RB^{(1)}[k, 1, kq_2]$ 和满足 § 1(i) (ii) 据作法显然。任给 τ 中的两元素 x 和 x' ($x \neq x'$)，若 $P_{\sigma\sigma'}^{\sigma\sigma'}(x)$ 和 $P_{\sigma\sigma'}^{\sigma\sigma'}(x')$ 相等或者在某个 $b_{r\beta}$ 中相遇，那么 x 和 x' 在 S_1 中相遇一次，在 S_2 中不相遇；而若 $P_{\sigma\sigma'}^{\sigma\sigma'}(x)$ 和 $P_{\sigma\sigma'}^{\sigma\sigma'}(x')$ 在某个 $b_{a\beta}$ 中相遇 ($a \in E(r-1)$)，那么它们在 S_2 中相遇一次，在 S_1 中不相遇 (参阅 § 7(ii))。由此知 S 也满足 § 1(iii)。定理证毕。

§ 18. 【定理】若 $q_2 > 0, 1 + q_2 \in RB(k, 1)$ ， $n = q_1 + (k-1)q_3 \in RB_{q_1}(k, 1)$ ， $q_3 \in RT(k)$ ，则 $q_1 + q_2 q_3 \in RB_*(k, 1)$ 。

证明：1. 令 $\tau = \tau'(q_1) \cup \sigma(q_2)\sigma'(q_3)$ ， $\tau'' = \{a\} \cup \sigma(q_2)$ ，取 τ'' 的元素构成 $RB'[k, 1, 1 + q_2]$ ；将其中的区组编号成 $b_{r\beta}$ ，前一足码相同的区组处在同一行中，并命 $b_{r\beta}$ 包含元素 $\{a\}$ ($a \in E(r)$ ， $\beta \in E(n)$ ， r 是行的总数， n 是每行的区组数)。

根据每一 $b_{r\beta}$ ($a \in E(r)$)，取元素集 $\{x, y; x \in \tau', y \in \sigma\sigma', P_{\sigma\sigma'}^{\sigma\sigma'}(y) \in b_{r\beta}\}$ 以之构成 $RB^{(2)}_{q_1}[k, 1, n]$ ，包含 τ' 的元素构成的 $RB''[k, 1, q_1]$ 。将 $RB^{(2)}$ 中不包含 RB'' 的区组的行编号记为 $k_{r\beta}$ ，包含 RB'' 的区组的行在取去这些区组后所

剩下的部分编号记为 $h'_{\alpha\delta}$, RB'' 的行编号记为 $h''_{\delta}(r \in E(q_3), \delta \in E(r'), r'$ 是 RB'' 的行的总数)。取 τ 中元素构成的设计 S_1 :

$$S_1 = \bigcup_{\delta \in E(r)} \left(\bigcup_{h_{\delta}'' a \in E(r)} h'_{\alpha\delta} \right),$$

以其中每个形如 $\bigcup_{h_{\delta}'' a \in E(r)} h'_{\alpha\delta}$ 的区组集组成一新的行, 它满足 RB 的行的条件。

2. 又取 σ' 的元素作成 $RT[k, q_3]$ 。根据每一组 $b_{\alpha\beta}(a \in E(r), \beta \in E(n-1))$ 构造 $(b_{\alpha\beta}, RT)$, 并将其中的行编号成 $h'''_{\alpha\beta r}(r \in E(q_3))$ 。

取以 τ 中元素构成的设计 S_2 :

$$S_2 = \bigcup_{\gamma \in E(q_3)} \left(\bigcup_{a \in E(r)} \bigcup_{h_{\alpha r} \beta \in E(n-1)} h'''_{\alpha\beta r} \right),$$

令其中每个形如 $\left(\bigcup_{h_{\alpha r} \beta \in E(n-1)} h'''_{\alpha\beta r} \right)$ 的区组集组成一新的行, 从 § 7(iii) 容易看出, 这样的行也满足 RB 的行的条件。

3. 令 $S = S_1 \cup S_2$, 则 S 是 $RB_{\alpha}[k, 1, q_1 + q_2 q_3]$ 。它包含 $RB^{(\alpha)}_{q_1}[k, 1, n]$ 、 $RB''[k, 1, q_1]$ 并满足 § 1(i)(ii) 据作法显然。任给 τ 中的两元素 x 和 $x'(x \neq x')$, 可得 (参阅 § 7):

① 若 x 和 $x' \in \tau$, 则它们在 RB'' 相遇恰一次, 在 S 的其他部分不相遇;

② 若 $x \in \tau', x' \in \sigma\sigma'$, 则它们在某个 $h_{\alpha r}$ 相遇恰一次, 在 S 的其他部分不相遇;

③若 x 和 $x' \in \sigma\sigma'$, $P_{\sigma}^{\sigma\sigma'}(x) = P_{\sigma}^{\sigma\sigma'}(x')$ 或 $P_{\sigma}^{\sigma\sigma'}(x)$ 与 $P_{\sigma}^{\sigma\sigma'}(x')$ 在 b_{α} 相遇, 则 x 和 x' 在 $RB^{(\alpha)}$ 相遇恰一次, 在 S 的其他部分不相遇;

④若 x 和 $x' \in \sigma\sigma'$, $P_{\sigma}^{\sigma\sigma'}(x)$ 与 $P_{\sigma}^{\sigma\sigma'}(x')$ 在 $b_{\alpha\beta}$ 相遇 ($\beta \in E(n-1)$), 则 x 和 x' 在 $(b_{\alpha\beta}, RT)$ 相遇恰一次, 在 S 的其他部分不相遇。

由上知 S 满足 §1(iii), 定理证毕。

(六) $k=3$, $\lambda=1$ 的 RB

§19. 【引1】若素数幂 $p^a = 1 + bt$ (t 是正整数), 则 $p^a \in RFY_1(3, 1, 2)$ 。

证明: 依 §10, 取 $GF(p^a)$ 为 K , $H_1 = \{1, \theta, \theta^2, -1, -\theta, -\theta^2\}$, $\theta = g^{2t}$ (g 是元根)。显然有 $\theta^3 = 1$, $\theta^2 + \theta + 1 = 0$ 。

命集 $\tau' = E(2)K$, 取其区组集 FS_1 :

$$FS_1: [(1, 1) (1, \theta) (1, \theta^2)], [(1, -1) (2, \frac{\theta+1}{\theta-1}) (2, -\frac{\theta+1}{\theta-1})], [(1, -\theta) (2, \theta^2 \frac{\theta+1}{\theta-1}) (2, -\theta^2 \frac{\theta+1}{\theta-1})], [(1, -\theta^2) (2, \theta^2 \frac{\theta+1}{\theta-1}) (2, -\theta^2 \frac{\theta+1}{\theta-1})]$$

容易验证, FS_1 是 $FE[3, 1, 2, 1, p^a]$ 。

令 $b = [\{a\} (1, 0) (2, 0)]$, 据 §13 定理可得 $FY_1[3, 1, 2, p^a] = \langle FS_1, A_1 \rangle \cup b$, 其元素属于 $\tau = \{a\} \cup \tau'$ 。因为 FY_1 本身满足 §15 的甲种行的

条件, 所以得到的且是 RFY_1 。

【引2】若素数幂 $p^a = 1 + \theta t$ (t 是正整数), 则 $p^a \in RFY_0(3, 1, 3)$ 。

证明: 仍取引1中的 K 和 H_1 。命 $\tau = MK$ (M 是阶为3的剩余模), 取其区组集 S_1 和 S_2 :

$S_1: [(0, 1)(0, \theta)(0, \theta^2)], [(0, -1)(1, -\theta)(2, -\theta^2)]$; $S_2: [(0, 1)(1, \theta)(2, \theta^2)]$ 。

容易验证, $FS_1 = S_1 \cup S_2$ 是 $FE = [3, 1, 1, 3, p^a]$ 。

令 $b = [(0, 0)(1, 0)(2, 0)]$, 据§13定理可得 $FY_0[3, 1, 3, p^a] = \Phi_M(\langle FS_1, A_1 \rangle) \cup b = \Phi_M(\langle S_1, A_1 \rangle) \cup \Phi_M(\langle S_2, A_1 \rangle) \cup b$ 。这里 $\Phi_M\langle S_1, A_1 \rangle \cup b$ 满足§15的甲种行的条件, 而 $\Phi_M\langle S_2, A_1 \rangle$ 中的每个区组满足乙种行的条件, 所以得到的且是 RFY_0 。

【命题】若素数幂 $p^a = 1 + bt$ (t 是正整数), 则 $1 + 2p^a \in RB(3, 1)$ ①, $3p^a \in RB(3, 1)$ 。

① 例如当 $p^a = 7$ 时可得 $RB(3, 1, 15)$, 这是由Kirkman提出而引起人们注意的第一个 RB 。它有7个互不同构的解, 而对于同样参数的 B , 则有90个互不同构的解【7】【8】【9】。Sylvester 提出的下面的问题尚未解决: ②对同一元素集可否构造13个 $RB(3, 1, 15)$ 使其不包含相同的两个组 (不考虑组内元素的次序) 【10】【11】。Cayley 对于 B 考虑同样的问题, 指出当 $v=7$ 时不存在 $v-2$ 个不包含两个相同组的 $B(3, 1, v)$; 而当 $v=15$ 时不存在循环性的解【11】【12】。作者已能证明, 对于 Cayley 问题, 1. $v=7$ 时至多可构造3个不包含两个相同的 $B(3, 1, 7)$; 2. 对 v 的相当一类的数字解存在, 如适合下式的 v 即具有循环性的解: $v = 2 + \prod p_i$, 素数 $p_i \equiv 7 \pmod{8}$ 。——陆家羲注。

② 陆家羲著此文后9年该问题已解决——本文作者注。

证明：据上面的两个引及§15即得。

§20. 设 $R = \prod p_i$ (p_i 是奇素数)，若对
 $i \in E(S)$

每一 $GF_i(p_i)$ ，存在元素 ξ_i ，使方程(6)和(7)对整数 α, β, γ 无解：

$$\xi_i(\xi_i - 1)(\xi_i + 1) = 0, \quad (6)$$

$$\xi_i^\alpha \left(\frac{\xi_i - 1}{2} \right)^\beta \left(\frac{\xi_i + 1}{2} \right)^\gamma = -1. \quad (7)$$

这事实我们用 $R \in C_1$ 来表示。

【命题】若素数 $p = 2^n h + 1$ (n 是正整数， h 是奇数)，则 $p \in C_1$ 的充要条件是，存在整数 ξ ， $p - 1 > \xi > 1$ ，使得 $\xi, \frac{\xi - 1}{2}$ 和 $\frac{\xi + 1}{2}$ 都是模 p 的

2^n 次剩余，即下面的同余方程组有解：

$$x_1^{2^n} \equiv \xi \pmod{p}, 2x_2^{2^n} \equiv \xi - 1 \pmod{p},$$

$$2 \cdot x_3^{2^n} \equiv \xi + 1 \pmod{p}.$$

证明：以同构的阶为 p 的剩余类环来表现 $GF(p)$ 。关于方程 (6) 的条件是没有问题的。

(7) 式等价于

$$\alpha \text{ind} \xi + \beta \text{ind} \frac{\xi - 1}{2} + \gamma \text{ind} \frac{\xi + 1}{2} \equiv 2^{n-1}h \pmod{2^n h}.$$

此式无解当且仅当 $\text{ind} \xi, \text{ind} \frac{\xi - 1}{2}$ 和 $\text{ind} \frac{\xi + 1}{2}$ 含有

因子 2^n 。命题由此即属显然。

【例1】根据上述命题及二次同余理论，可以证明下面形式的素数 $p \in C_1$ ：

$$p \equiv 31, 47, 55 \pmod{56} \quad (\text{存在 } \xi = 8),$$

$$p \equiv 11, 19 \pmod{20} \quad (\text{存在 } \xi = 9)。$$

【例2】 C_1 中小于100的素数可由指数表查得，列表于下：

素数	11	19	23	29	31	43	47	59	61	67	71	79	83
最小的 ξ	9	9	2	20	8	4	2	7	25	4	2	9	7

§ 21. 【命题】若 $q = 3$ 或 9 , $R \in C_1$, 则 $R \in RFY_q(3, 1, 36)$ 。

证明：依 § 10, 由分解式 $R = \prod_{i \in E(s)} q_i$ 确定环

K 。从每个 G_j 确定元素 $w_j (j \in E(2^s - 1))$ ； w_j 在 $GF_i(p_i)$ 上的投影若不是据 G_j 的定义为 0 即等于在 § 20 中定义的某一 $\xi_i (i \in E(S))$ 。令 H'_j 是元素 $w_j, \frac{w_j - e_j}{2e_j}$ 和 $\frac{w_j + e_j}{2e_j}$ 在 G_j 内的生成群，即

为形如下式的元素集：

$$w_j^{\alpha} \left(\frac{w_j - e_j}{2e_j} \right)^{\beta} \left(\frac{w_j + e_j}{2e_j} \right)^{\gamma} \quad (\alpha, \beta, \gamma \text{ 是任意整$$

数)。

由于 $R \in C_1$, $-H'_j$ 是 H'_j 的不同的陪集，取 § 10 中定义的 H_j 为 H'_j 和 $-H'_j$ 的和集。

命 $\tau = M \cdot K$, M 是阶为 36 的剩余模。取 τ 中元

素的区组集 S'_j 和 S^2_j :

S^1_j : $[(2, -w_j)(2, e_j)(6, -e_j)]$, $[(6, w_j)(33, e_j)(15, -e_j)]$;

S^2_j (每组的第一个元素在 K 上的投影是 $-w_j$, 第二个元素是 e_j , 第三个元素是 $-e_j$. 下面只写出在 M 上的投影):

组序: $b^1_j \ b^2_j \ b^3_j \ b^4_j \ b^5_j$

组内元素: $[4, 5, 7][8, 13, 21][10, 17, 29]$
 $[12, 18, 32][16, 27, 1]$

可以验证区组集 $FS_j = \langle S^1_j, H'_j \rangle \cup \langle S^2_j, H_j \rangle$ 满足§10中的性质 (i) 和(ii), 由此得

$$\begin{aligned} FE[3, 1, 1, 36, R] &= \bigcup_{j \in E(2^s - 1)} FS_j \\ &= \bigcup_{j \in E(2^s - 1)} (\langle S^1_j, H'_j \rangle \cup \langle S^2_j, H_j \rangle). \end{aligned}$$

取集合 $\tau'(q) \cup MG_{11}$, 并依§17和§19构成 $RB_q [3, 1, 36 + q]$ 包含 τ' 的元素构成的 RB'

$[3, 1, q]$. 令 $S = \Phi M \left(\bigcup_{j \in E(2^s - 1)} \langle FS_j, A_j \rangle \right)$

$\cup RB_q$, 从 S 中取出 RB' 后所得的是 $FY_q [3, 1, 36, R]$ (§13), FY_q 的区组可以由下面的方法组成甲种行 h_z 和乙种行 h' :

$$\begin{aligned} h_z = h_{z+18} &= \varphi_z \left(\bigcup_{j \in E(2^s - 1)} \langle FS_j, A_j \rangle \right) \\ &\cup \varphi_{z+18} \left(\bigcup_{j \in E(2^s - 1)} \langle FS_j, A_j \rangle \right) \cup h'', \end{aligned}$$

这里 $z \in M$, h'' 是 RB_q 中不含 RB' 的组的

某一行, 而 h' 是 RB_q 含 RB' 的组的任一行所剩下的区组集。因所得的 FY_q 满足 §15 (ii), 定理即得证。

§22. 【命题】若 $q=3$ 或 9 , $R \in C_1$, 则 $R \in RFY_{q+12}(3, 1, 36)$ 。

证明: 取集合 $\tau'(q) \cup MK$, 并按 §21 的方法以之作成 $RFY_q[3, 1, 36, R]$ (M 和 K 的意义同 §21)。命 $\tau''(12) = \{\hat{1}, \hat{2}, \dots, \hat{12}\}$ 。任取 K 中的一对非 0 元素 a 和 $-a$, 假设 a 和 $-a \in G_{j_0}$ ($j_0 \in E(2^5 - 1)$), 在 RFY_q 的每个 h_z 中取去区组集 S_z :

$$S_z: \varphi_z(\langle b^1_{j_0}, a \rangle), \varphi_{z+18}(\langle b^1_{j_0}, a \rangle), \varphi_z(\langle b^1_{j_0}, -a \rangle), \varphi_{z+18}(\langle b^1_{j_0}, -a \rangle), \varphi_z(\langle b^5_{j_0}, a \rangle), \varphi_{z+18}(\langle b^5_{j_0}, a \rangle), \varphi_z(\langle b^5_{j_0}, -a \rangle), \varphi_{z+18}(\langle b^5_{j_0}, -a \rangle) \textcircled{1},$$

代之以由表 1 所示的区组集 S'_z 。取代后 h_z 变成 h'_z , 对于集 $\tau = \tau' \cup \tau'' \cup MK$, h'_z 满足 §15 的甲种〔表 1〕行的条件。 RFY_q 在作了上述改变后再添入下面所示的 6 个乙种行 h_u'' ($u \in E(6)$), 便变成了 $RFY'_{q+12}[3, 1, 36, R]$ (参阅 §9) :

① 参阅 §21, 易见 $\langle S^2_{j_0}, H_{j_0} \rangle, A_{j_0} \rangle = \langle S^2_{j_0}, G_{j_0} \rangle = \bigcup_{u \in E(5)} \langle b^u_{j_0}, G_{j_0} \rangle$. 因此 $S_z \subset \varphi_z(\langle S^2_{j_0}, H_{j_0} \rangle, A_{j_0} \rangle) \cup \varphi_{z+18}(\langle S^2_{j_0}, H_{j_0} \rangle, A_{j_0} \rangle) \subset \varphi_z(\langle FS_{j_0}, A_{j_0} \rangle) \cup \varphi_{z+18}(\langle FS_{j_0}, A_{j_0} \rangle) \subset h_z$. ——陆家羲注。

$$h_u'' = \bigcap_{z \in E(6)} (\varphi_{6z+u}(b') \cup \varphi_{6z+u}(b'')),$$

$$b' = [(16, -aw_{j_0}) (27, a) (1, -a)],$$

$$b'' = [(29, -aw_{j_0}) (18, a) (8, -a)],$$

这里 $6z+n \in M$ 。

注意：这里由 RFY_q 变成 $RFY_{q'+12}$ 的方法可名之为分析法。实际上表1是这样设计的：先将于 h_1 中取出的 S_1 析成12个 $k=2$ 的区组，然后在每个 h_z ($z \in E(18)$) 中作相对应的分析①。再在这些析成的区组上配上 τ'' 的元素使之满足甲种行和 §9(ii) 的条件。元素 $\hat{1}$ 在表1所配入的区组可简记为 $\{(7+4z, 8+4z), (18+4z, 21+4z), z \in M\}$, 余类推。

§23. 【命题】若 $q=3$ 或 9 , $R \in C_1$, 则 $R \in RFY_{24}(3, 1, 36)$ 。

证明：证明与§22类似，这里取集合 $\tau'' = \{\hat{1}, \hat{2}, \dots, \hat{24}\}$ 。在 $RFY_q[3, 1, 36, R]$ 的 h_z 中除了取去§22中指出的 S_z 外，再取去将 S_z 的表式中的 b'_{j_0} 和 $b^5_{j_0}$ 分别改为 $b^2_{j_0}$ 和 $b^3_{j_0}$ 后的区组集。将 h_z 中取出的区组分析成 $k=2$ 的区组集 S''_z , $S''_z = \varphi_z(S''_0) \cup \varphi_{z+18}(S''_0) \cup \varphi_z(\langle S''_0, -e_{j_0} \rangle) \cup \varphi_{z+18}(\langle S''_0 - e_{j_0} \rangle)$ ②，其中

① 因此使 S_1' 中元素的在 M 上的投影加以 z , 即得到 S_{1+z} 的属于 MK 的元素 (见表1)。——陆家羲注。

② 本节 φ 下的足码均是阶为 $3b$ 的剩余模 M 的元素。——陆家羲注。

$$S''_0: [(3, a) (4, -aw_{j_0})], [(17, a)(28, -aw_{j_0})], \\ [(25, a)(27, -a)], [(31, a)(5, -a)], \\ [(1, a)(16, aw_{j_0})], [(8, -aw_{j_0})(11, -a)].$$

τ'' 的元素可以配入这些区组。 $\hat{1}$ 所配入的区组为 $\{(7+4z, 9+4z), (8+4z, 10+4z)\}$, $\hat{2}$ 所配入的区组为 $\{(1+4z, 11+4z), (2+4z, 12+4z)\}$, $\hat{3}$ 所配入的区组为 $\{(1+4z, 2+4z), (4+4z, 15+4z)\}$, $\hat{4}$ 所配入的区组为 $\{(1+4z, 4+4z), (3+4z, 18+4z)\}$, 余仿此 ($z \in M$)。补充12个乙种行。其中3行为 $h_u^{(1)} = \bigcup_{z \in E(1)}$

$\varphi_{3z+u}(b)$, 又3行为 $h_u^{(2)} = \bigcup_{z \in E(12)} \varphi_{3z+u}(\langle b, -e_{j_0} \rangle)$, 这里 $u \in E(3)$, $b = [(8, aw_{j_0}) (21, a) (13, -a)]$ 。其余6行为 $h_{u,u}^{(3)} = \bigcup_{z \in E(12)}$

$\varphi_{18z+6u+u'}(S)$, 这里 $u \in E(3)$, $u' \in E(2)$, $S = b' \cup \varphi_1(b') \cup \varphi_4(b') \cup b'' \cup \varphi_1(b'') \cup \varphi_4(b'')$, $b' = [(10, -aw_{j_0}) (17, a) (29, -a)]$, $b'' = [(5, -aw_{j_0}) (34, a) (22, -a)]$ 。

§24. 【引】若 $q=3$ 或 9 , $R \in C_1$, $q'=12t$, $t \leq R-2$, $q+q' \in RB(3,1)$, 则 $q+q'+36R \in RB_{q+q'}(3,1)$ 。

证明：据§15中的定理，只须证明 $R \in RFY_{q+q'}(3, 1, 36)$ 。当 $t=0$ 时已在§21中证明。当 $t=1$ 和 2 时也已在§22和§23中证明，此证明基于选定某一对元素 a 和 $-a$ 而分析 $RFY_q[3, 1, 36, R]$ 。由于不同的 a 和 $-a$ 的选取共有 $\frac{R-1}{2}$ 种，又在选取一对 a 和 $-a$ 后可再选取另一对作分析。这样，若 t 是偶数选取 $\frac{t}{2}$ 对，若 t 是奇数选取 $\frac{t+1}{2}$ 对，就可构成 $RFY_{q+q'}[3, 1, 36, R]$ 。

【定理】 $v \in RB(3, 1)$ 的充要条件是 $v \equiv 3 \pmod{6}$ 。

证明：必要性由 (1) 和 (2) 即得，为了证明充分性，将 v 写成 $v = u + 36R'$, $u \leq 33$ 。

1. $R' \geq 43$ 的情形。

据§20，写出 C_1 中整数的序列：43, 47, 61, 79, 103, 131, 167, 211, 271, 359, 473，则恒存在正整数 n 和序列中的整数 R_1, R_2 ，使得下面的两个式子成立：

$$11^n R_1 \leq R' < 11^n R_2, 3(R_2 - R_1) \leq R_1 - 1.$$

因此在将 v 写成 $v = q + q' + 36(11^n R_1)$ 后 ($q = 3$ 或 9)，据引可归结出下面的情形。

2. $R' < 43$ 的情形。

除却 $v = 69$ ，这种情形在前文中都可以直接找到构造公式。例如，将 v 写成 $v = 3u$ ，若 u 不

是素数可利用§17, 若 u 是形为 $1+6m$ 的素数可利用§19, 在 u 是形为 $5+6m$ 的素数的情形可利用§18、§19和§24引 (参阅附表一)。

下面给出 $RB[3, 1, 69]$ 的一种构造。命 $\tau(69) = \tau' \cup M'M$, $\tau' = \{a\} \cup M'\sigma$, M' 是阶为 2 的剩余模, M 是阶为 27 的剩余模, $\sigma = \{\hat{1}, \hat{2}, \dots, \hat{7}\}$ 。取 τ' 的元素构成 $RB'[3, 1, 15]$, 其中的行以 \tilde{h} 表示。于是可将 RB 的 34 行编号为: h_z ,

$\begin{matrix} (1) & (2) & (3) \\ h_u & h_u & h \end{matrix}$ ($z \in M, u \in E(3)$); 行的具体构造如下:

$$h_z = \varphi_z(h_0), h_0 = b_{z' \in M'} \bigcup S_{z'}, b = [(0, 10) (1, 10)a],$$

$$\begin{aligned} S'_{z'}: & [(1+z', 14)(1+z', 15)(z', 2)], \\ & [(z', 5)(1+z', 22)(z', 11)], [(1+z', 18)(1+z', 21)(z', 12)], [(z', 7)(z', 9)(z', 24)], \\ & [(z', 1)(1+z', 25)(z', \hat{1})], [(1+z', 16)(z', 20)(z', \hat{2})], [(z', 3)(1+z', 8)(z', \hat{3})], \\ & [(1+z', 17)(z', 19)(z', \hat{4})], [(z', 4)(1+z', 23)(z', \hat{5})], [(z', 6)(1+z', 13)(z', \hat{6})], \\ & [(1+z', 26)(z', 0)(z', \hat{7})], \end{aligned}$$

$$\begin{matrix} (1) \\ h_u \end{matrix} = \bigcup_{\substack{z \in M' \\ t \in E(9)}} [(z', 3t+u)(z', 5+3t+u)]$$

$$(z', 13 + 3t + u) \supseteq \bigcup \tilde{h},$$

$$(2) \quad \bigcup_{\substack{h_v = z' \in M \\ t \in E(9)}} [(z', 3t + u)(z', 4 + 3t + u)]$$

$$(z', 11 + 3t + u) \supseteq \bigcup \tilde{h},$$

$$\bigcup_{\substack{h^{(3)} = z' \in M' \\ t \in E(9)}} [(z', t)(z', 9 + t)(z', 18 + t)]$$

$$\bigcup \tilde{h}.$$

(以下各部分请读附录)

陆家羲的这一重大成果由于历史原因未能获得正式发表。上海交通大学的沈灏同志1985年底到加拿大多伦多大学跟随曼德尔逊教授学习组合设计理论，有机会与国外学者交流。他曾为准备“陆家羲学术工作评审会议”系统研究过陆的论文，因而向国外学者介绍了上述成果。在本书中多次提到的威尔逊，任美国加利福尼亚州理工学院教授，是1971年解决科克曼女生问题的学者之一。沈灏把陆家羲领先十年解决此问题的事告诉威尔逊教授，“他非常感兴趣，并且很想知道陆老师所用的方法”（引自沈灏致内蒙古数学会理事长、内蒙古大学陈杰教授的信），国外也希望将此文译成英文发表。

所以，在组合设计的发展史上应当留下这样的记载：历时百余年的、著名的科克曼女生问题，60年代初期由中国一位中学教师陆家羲首先

解决，但他的论文未能发表；1971年雷·乔得赫里和威尔逊合作，首先发表论文解决了这一问题。他们各自独立的、首创性的工作将同样得到科学和历史的尊重。为得到这个结论，本书分节全文引用了陆文，并以此纪念陆家羲逝世五周年。

十、斯坦纳系的 相交性问题



定义在同样的 v -集上已知的两个同类型的斯坦纳系 $S(t, k, v)$ ，它们可能有多少个区组是共同的？能否找出这样的两个系列，它们没有一个区组是共同的？如果这样的系列存在，那么最多能找到多少个？这类问题在斯坦纳系还处于襁褓时代就已引起了研究者的兴趣。例如凯莱还是在1850年就已证明了，对于一个已知的7元集，存在且仅存在两个不相交斯坦纳三连系²⁹⁾；科克曼在这同一年发现了不相交9阶斯坦纳三连系最多有7个。但是在这个领域内获得的具有实质性的成果，才不过是近二十年来的事情。

同一集 X 上的两个斯坦纳系 $S(t, k, v)$ 如果没有一个区组是共同的，那么它们是不相交(disjoint)的，或称互斥的。本文用 $d(t, k, v)$ 表示两两不相交的 $S(t, k, v)$ 的最大个数，用 $d(v)$ 表示两两不相交的 $S(v)$ 的最大个数，用 $d^*(v)$ 表示不相交且同构的 $S(v)$ 的最大个数。

由于每个 $S(t, k, v)$ 有 $\binom{v}{t} / \binom{k}{t}$ 个区组，

一个 v -集共有 $\binom{v}{k}$ 个 k -子集, 故

$$d(t, k, v) \leq \binom{v-t}{k-t} \quad (10.1)$$

(10.1)式取等号时, 所有 $\binom{v-t}{k-t}$ 个 $S(t, k, v)$ 叫做不相交斯坦纳系大集。

对斯坦纳三连系还可以做这样的分析: 由于 v -集 X 所能构成的全部不同的三元组的总数是

$$\binom{v}{3} = v(v-1)(v-2)/6, \text{ 而一个 } S(v) \text{ 共有 } b =$$

$v(v-1)/6$ 个不同的三元组, 于是存在可能

$$d(v) = \binom{v}{3} / b = v-2 \quad (10.2)$$

满足(10.2)的所有 $v-2$ 个 $S(v)$ 叫做不相交斯坦纳三连系大集。在(10.1)式中取 $k=3, t=2$, 也得到(10.2)。我们已知 $d(7)=2$, 这说明 7 阶斯坦纳三连系不满足(10.2), 它的两个 $S(7)$ 虽不相交, 却不能构成大集; 而 $d(9)=7$, 即 7 个互不相交的 $S(9)$ 可以构成一个大集。

例, $X = \{1, 2, \dots, 9\}$, 列出 7 个不相交的 $S(9)$ 所构成的大集。

先列出 7 个方阵 (它们须满足一定关系, 不是随意给出的):

$$\begin{pmatrix} 1 & 2 & 4 \\ 3 & 7 & 8 \\ 9 & 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 8 \\ 9 & 4 & 3 \\ 7 & 6 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 5 \\ 9 & 8 & 3 \\ 4 & 7 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 9 \\ 7 & 4 & 3 \\ 5 & 8 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 6 & 9 \\ 7 & 8 & 5 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 6 \\ 3 & 5 & 7 \\ 4 & 8 & 9 \end{pmatrix} \begin{pmatrix} 1 & 2 & 7 \\ 3 & 4 & 6 \\ 5 & 9 & 8 \end{pmatrix}$$

我们先把第一个方阵按三横行、三纵列和方阵的行列式的展开式中六个乘积（不考虑它们的符号）的顺序排出12个三元组。

$\{1, 2, 4\}, \{3, 7, 8\}, \{9, 5, 6\}, \{1, 3, 9\},$
 $\{2, 7, 5\}, \{4, 8, 6\}$

$\{1, 7, 6\}, \{2, 8, 9\}, \{4, 3, 5\}, \{4, 7, 9\},$
 $\{2, 3, 6\}, \{1, 8, 5\}$

这就构成了一个 $S(9)$ ；用同样的方法还可以得到另外 6 个 $S(9)$ 来，它们都是两两不相交的，共有 84 个不同的三元组。这 7 个不相交的 $S(9)$ 构成了 9 阶斯坦纳三连系大集。

对给定的正整数 v ，若存在 v 阶斯坦纳三连系（或当 $v = 6n + 3$ 时所称的科克曼三连系）大集，则这种大集也可能不止一个。比如对 $v = 9$ ，除去上例给出的大集外，还有如下的另一个：

$$\begin{pmatrix} 1 & 3 & 9 \\ 2 & 7 & 5 \\ 4 & 8 & 6 \end{pmatrix} \begin{pmatrix} 1 & 9 & 2 \\ 7 & 4 & 5 \\ 8 & 6 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 7 \\ 4 & 8 & 5 \\ 6 & 3 & 9 \end{pmatrix} \begin{pmatrix} 1 & 7 & 4 \\ 8 & 6 & 5 \\ 3 & 9 & 2 \end{pmatrix} \begin{pmatrix} 1 & 4 & 8 \\ 6 & 3 & 5 \\ 9 & 2 & 7 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 8 & 6 \\ 3 & 9 & 5 \\ 2 & 7 & 4 \end{pmatrix} \begin{pmatrix} 1 & 6 & 3 \\ 9 & 2 & 5 \\ 7 & 4 & 8 \end{pmatrix}$$

可以验证，集 $X = \{1, 2, \dots, 9\}$ 不存在这样的置换，使得第一个大集的全部三连系通过这一置换

变成第二个大集的全部三连系；换言之，这两个大集是不同构的。

由上边的讨论，易知对 $v \geq 3$, $v \equiv 1, 3 \pmod{6}$ 有

$$1 \leq d^*(v) \leq d(v) \leq v-2 \quad (10.3)$$

在斯坦纳系诸多性质之中相交性占据着显著的地位；相交性的特例是交集为零，即不相交，又处在十余个相交性问题之首。所谓“大集问题”，就是大集的存在问题；所谓“大集定理”，就是要证明它存在的必要充分条件。

法国数学家贝斯在1917年曾首次说明了：恰有两个不同构的9阶斯坦纳三连系大集^[51]，这一点1974年被重新证实^[52]。本节所举的 $S(9)$ 的两个大集的例子，正是贝斯所给出的。而克雷默和梅斯纳在1975年在计算机上用穷举法证明了：恰有两个不同构的13阶斯坦纳三连系大集^[53]。

关于斯坦纳四连系和其他斯坦纳系的不相交性问题，在罗沙1980年的综述文章“斯坦纳系的相交性”^[54]中已作了较详尽的介绍；在这篇文章里还有“规定相交的斯坦纳系”的丰富内容，如准不相交斯坦纳三连系、共同区组为已知数的斯坦纳系、交于子系列的斯坦纳系等；以及相关的问题： $\lambda \geq 1$ 的不相交三连系、设计 $S_\lambda(t, k, v)$ 的存在性和正交 (perpendicular, 旧称 orthogonal) 斯坦纳系诸问题。在后一方面，我国组合数学工作者朱烈教授曾得到：当 n 与6互素时，存在3

个两两正交的 $S(2, 3; 2^n - 1)$ 。特别地, 对于 $n = 7$, 他作出了6个两两正交的 $S(2, 3; 127)$ ^[24]。

这里, 我们仅就不相交斯坦纳三连系大集问题, 追溯它的历史和数学思想的发展过程。

科克曼不仅是女生问题的提出者、斯坦纳系的首创者, 他也是大集问题的最早提出者。我们已谈到, 1850年他证明了 $d(9) = 7$ 。对于 $d(13)$ 和 $d(15)$, 问题的困难程度陡增, 他获得了 $d(13) \geq 3$, $d(15) \geq 2$, 就是找到了解决这类问题的起点或下界。如果能逐步提高下界, 那么可望达到 $d(v) = v - 2$ 。以后有些数学家即用提高下界的方法朝这个方向前进。同时, 他还定义了 $d(v, n)$ (整数 n 满足 $0 \leq n \leq v(v-1)/6$), 表示可能构成的、两两具有 n 个共同区组的 $S(v)$ 的最大数目, 这也是规定相交的斯坦纳系问题的发轫之作, 他得到 $d(15, 5) \geq 15$, 也用先定下界的方法。然而, 时至今日, 对共同区组为已知数的斯坦纳系, 仍然所知无几。

在第三节里提到的“西尔沃斯特问题”, 即恰有13个不相交 $S(15)$ (或 $S_4(15)$) 构成一大集的猜想, 正是满足(10.2)式的, 它经过一百多年才被具体构造出来, 迄今仍是不相交科克曼三连系大集一个重要的脍炙人口的例证。

从19世纪50年代以来逐步形成的所谓斯坦纳三连系大集问题就是: 是否对所有的 $v \equiv 1, 3 \pmod{6}$, $v \geq 9$, 都有 $d(v) = v - 2$?

这里, $d(1)$ 没有意义, $d(3) = 3 - 2 = 1$ 是平凡的, 而 $d(7) = 2 < 5 = 7 - 2$, 故问题对 $v \geq 9$ 提出。

对于科克曼三连系 $S_K(v)$ 也有类似的问题。即若定义 $d_K(v)$ 为两两不相交的 $S_K(v)$ 的最大个数, 则科克曼三连系大集问题就是: 是否对所有的 $v \equiv 3 \pmod{6}, v \geq 9$, 都有 $d_K(v) = v - 2$? 这个推及一般的西尔沃斯特问题, 实际上就是猜测, 一定能够编出 $v - 2$ 个一般的科克曼女生问题的散步方案来。要证明它, 目前看来还是遥远的事。

本世纪前期, 数学家贝斯提出了一个猜想^[54], 即对任 $v \equiv 1, 3 \pmod{6}, v > 7$, 是否存在

$$d(v) \geq \frac{v-1}{2} \quad (10.4)$$

后来被称为“贝斯猜想”。它把不相交 v 阶斯坦纳三连系的最大数目的下界提高到刚超过 $v - 2$ 的一半, 直到1972年才有人基本证明了它, 并又向前跨出一步, 下文还要详述。

除此之外, 在直接证明一个个具体的 v 是否满足(10.2)式的方向上, 问题似乎显示出特殊的困难性。继凯莱证明 $d(7) = 2$ (1850), 科克曼证明 $d(9) = 7$ 之后, 西尔沃斯特^{[55][56]}: $d(9) = 7$ (1861), 瓦勒斯基^[57]: $d(9) = 7$ (1883), 贝斯^[58]: $d(9) = 7$ (1917), 依姆希^[59]: $d(9) = 7$ (1929), 至少有四位数学家重复了同一工作, 具体构造了无进展, 百余年间踏步不前, 这种逡巡

难进的状况持续到60、70年代，进入了斯坦纳系的现代研究时期。

1980年前，组合数学家多延、特林克、德尼斯顿、罗沙等人作出不少贡献。首先是继续研究提高下界的方法，1966、1967年有人算出 $d(31) \geq 6$ ⁽⁵⁹⁾⁽⁶⁰⁾，只知一般结果是对任奇整数 $n \geq 3$ ， $d^*(2^n - 1) \geq 2$ ，这些结果是平凡的。到1972、1973年，数学家们屡次重复 $d(v) = v - 2$ ($v \geq 9$) 这一猜想⁽⁶¹⁾⁽⁶²⁾。多延⁽⁶¹⁾在这一较长时间考虑的问题上取得了有意义的突破性的工作，他证明了贝斯猜想对任 $v \equiv 3 \pmod{6}$ 即令 $d(v)$ 被 $d^*(v)$ 代替也是对的。他得到

$$d^*(6m+3) \geq \begin{cases} 4m+1, & \text{若 } m \equiv 0, 2 \pmod{3} \\ 4m-1, & \text{若 } m \equiv 1 \pmod{3} \end{cases} \quad (10.5)$$

(10.5)式以直接构造法证明，应用了玻斯著名的结果⁽⁴³⁾。另外，

$$d^*(6m+1) \geq \begin{cases} m/2, & \text{若 } m \equiv 0 \pmod{2} \\ m, & \text{若 } m \equiv 1 \pmod{2} \end{cases} \quad (10.6)$$

(10.6)式也以直接法证明，依据斯科勒姆 (Th. Skolem) 的一个构造⁽⁶³⁾。这些结果是很不错的，对 $v \equiv 3 \pmod{6}$ 的情况，比贝斯猜想还进了一步。他还给出 $d(v)$ 的下界

$$d(2v+1) \geq d(v) + 2 \quad \text{对 } v \geq 7 \quad (10.7)$$

其推论为 $d(6m+1) \geq 2m-1$ 对 $m \equiv 1 \pmod{2}$

$$(10.8)$$

对式(10.5)所示下界, 后来的改进为^[64]:

$$d^*(6m+3) \geq 4m+2 \quad (10.9)$$

科兹格(A. Kotzig)^[65]又于1975年加强了不等式(10.8):

$$d(6m+1) \geq 3m+1 \quad \text{对 } m \equiv 1 \pmod{2} \quad (10.10)$$

至此, 贝斯猜想(10.4)除当 $v \equiv 1 \pmod{12}$ 外都是被证明过的了, 悬而未决的情况, 最小值是 $v = 37$ ^[64]。

沿着提高下界的道路能不能达到最终目的 $d(v) = v - 2$, 现在我们还不知道。已走过的路程虽然用去了百余年时间, 但目标似乎还很遥远。

但是, 在结果(10.7)中已包含了用较低阶的 v 来计算较高阶的 $v' = 2v + 1$, 即在研究下界时又用了递归的方法, 它暗示了一个新的途径。很快, 特林克^[62]1973年得出:

$$d(3v) \geq 2v + d(v) \quad \text{对 } v \geq 3 \quad (10.11)$$

$$\text{并立得 } d(3^m) = 3^m - 2 \quad \text{对 } m \geq 1 \quad (10.12)$$

这一简洁优美的递归构造显示了对于无穷多个 v 值, $d(v) = v - 2$ 也是成立的。

不久, 罗沙^[66]于1975年证得

$$d(2v+1) \geq v+1+d(v) \quad \text{对 } v \geq 7 \quad (10.13)$$

并进而获得: 如果 $d(v) = v - 2$, 则

$$d(2v+1) = 2v - 1 \quad (10.14)$$

特林克和罗沙的这两个递归定理在解决大集

问题的方法上别开生面,1976年特林克⁽⁶⁷⁾又得到若 $d(w) = w - 2$, 则

$$d(v(w-2)+2) = v(w-2) \quad (10.15)$$

对 v 尚有限制, 这里不详述了。

另一方面, 数学家们于1973、1974年开始用直接法计算满足 $d(v) = v - 2$ 的阶数较低的 v : 德尼斯顿⁽⁶⁸⁾算出 $v = 13, 15, 19, 21, 25, 31, 33, 43, 49, 61, 69$ 。上述科克曼三连系大集 $d_K(15) = 13$ 他是借助于计算机才找到的⁽⁶⁹⁾。斯端伯⁽⁷⁰⁾和威尔逊⁽⁷¹⁾得到 $v = 9, 25, 33, 49, 51, 73, 75, 81, 91, 105, 129, 153, 163, 169, 193, 201$ 满足 $d^+(v) = v - 2$ 。这是用他们的方法所得到的部分结果。

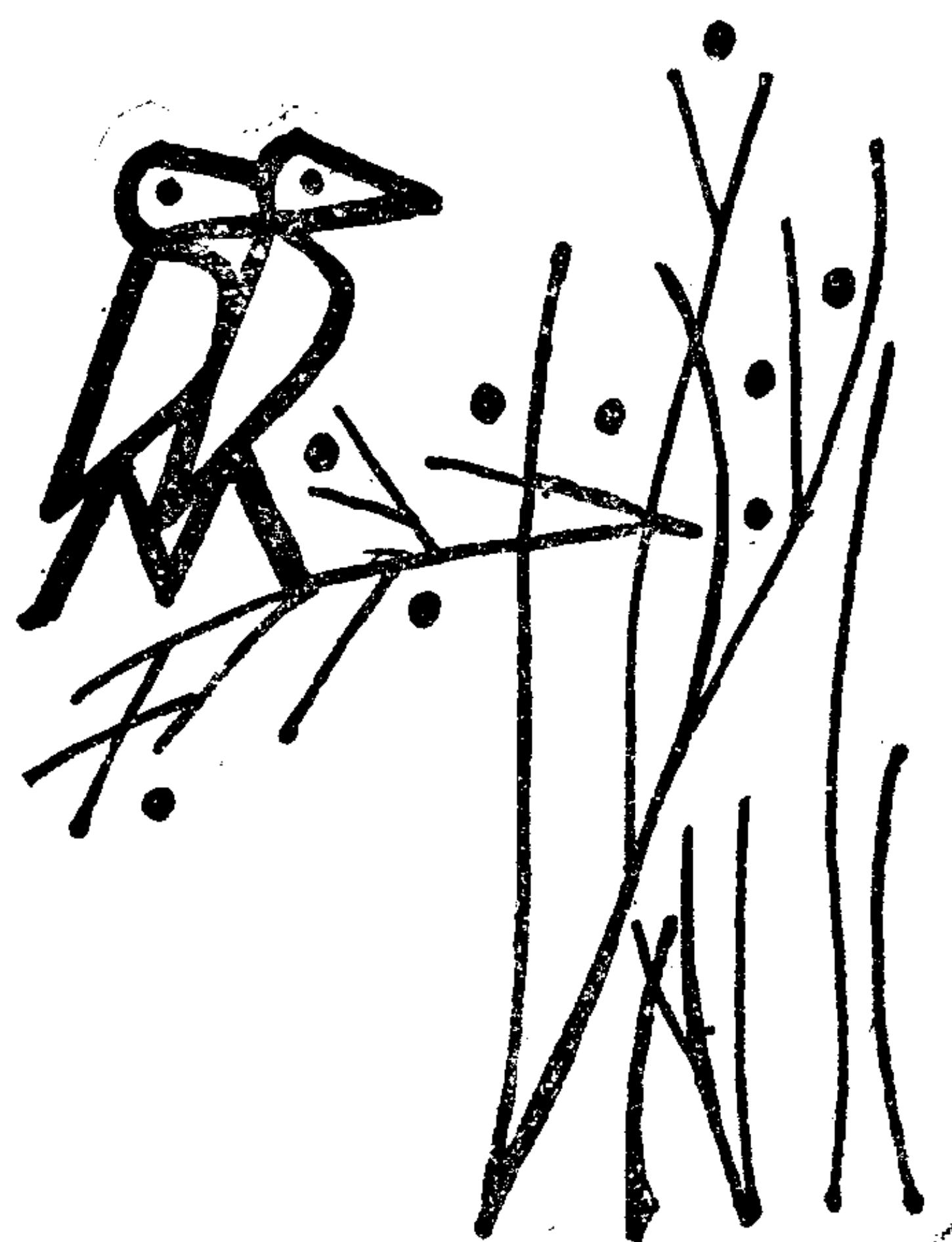
综上所述, 在1976年前, 对 $v \equiv 1, 3 \pmod{6}$, $9 \leq v \leq 205$, 除了 $v = 37, 85, 97, 109, 133, 141, 145, 157, 159$ ①, 181, 195之外, 方能满足 $d(v) = v - 2$ ⁽⁶⁴⁾。关于大集的存在问题, 包括(10.5)——(10.15)在内, 所得的结果还是比较零碎的, 对完全解决尚有很大差距, 实际上还没有找到一条能完全解决它的途径⁽⁶⁸⁾。

1976年后有五、六年时间, 这一问题的讨论显得有些沉寂。林德奈1981年5月在《组合论杂

① 注: 这是据文献〔54〕, 但是, 159一值写在这里可能有误。取 $v=19$, 三次运用(10.14)式, 得 $d(159) = 157$ 。姑录以备考。

志》上还说，它离解决还很远^[72]。但是，在世界组合学界没有料到的地方，突然有人宣告了这一大集问题的全部解决：1981年至1983年，设在美国加利福尼亚大学洛杉矶分校数学系的国际性刊物《组合论杂志》编辑部，陆续收到了一批题为“论不相交斯坦纳三元系大集”的论文。论文的作者是中国包头九中一个普通物理教师——陆家羲。

十一、不相交斯坦纳三连系 大集定理



1981年9月18日到1983年3月4日,《组合论杂志》编辑部陆续收到陆家羲“论不相交斯坦纳三元系大集 I—VI”^{[73], [74]} 的六篇英文论文。该杂志以100页的篇幅分两次予以发表,长达十余万字。他在论文中证明了这样的“大集定理”:

如果 $v \equiv 1, 3 \pmod{6}, v > 7$ 和 $v \notin \{141, 283, 501, 789, 1501, 2365\}$, 则 $d(v) = v - 2$ 。
(11.1)

这个定理主要由以下七个引理推出:

引理一^[62] 如果 $d(v) = v - 2$, 则

$$d(3v) = 3v - 2 \quad (11.2)$$

引理二^[66] 如果 $d(v) = v - 2$ 和 $v \geq 7$, 则

$$d(2v + 1) = 2v - 1 \quad (10.14)$$

引理三^[74, 文论 V] 如果 $d(n + 2) = n$, $n \equiv 11 \pmod{12}$ 和 $n \notin \{23, 47, 59, 83, 107, 167, 179, 227, 263, 299, 347, 383, 719, 767, 923, 1439\}$, 则

$$d(3n) = 3n - 2 \quad (11.3)$$

引理四 [73, 论文 I] 如果 $d(n+2) = n$, p 是素数, $p \equiv 7 \pmod{8}$ 或 $p \in \{5, 17, 19, 29\}$, $(p, n) \neq (5, 1)$, 则

$$d(2+pn) = pn \quad (11.4)$$

引理五 [73, 论文 I] 如果 n 是奇数, 存在着 12 个互相正交的阶为 n 的拉丁方, 而且 $d(1+2n) = 2n - 1$, 则

$$d(1+12n) = 12n - 1 \quad (11.5)$$

引理六 [74, 论文 IV] 如果 $d(1+4n) = 4n - 1$, n 是正整数 $p \in \{1, 2, 5\}$, 则

$$d(1+12pn) = 12pn - 1 \quad (11.6)$$

引理七 [47, 论文 V] 如果 $d(1+12n) = 12n - 1$, n 是奇数, $p \in \{7, 11\}$ 则

$$d(1+12pn) = 12pn - 1 \quad (11.7)$$

至此, 对 $v > 7$ 除六个值外, 猜想 $d(v) = v - 2$ 已宣告成立。

陆家羲在利用特林克^[62]和罗沙^[66]的成果时, 明确地表述成 (11.2)、(10.14) 这样简洁优美的形式。在前五篇论文中, 他独创了一系列的辅助设计, $AD, AD^*, AD^{**}, LD, LD^*$ 及辅助设计大集 LAD_1, LAD_2, LAD_3 , 它们本身也都可以作为独立的研究对象 (我国组合数学工作者康庆德教授就此曾写过一篇“ LD 设计的一个递归构造”^[65]), 在区组设计中具有一定的理论价值。他巧妙地引进了多种素数因子, 精心设计

了一个又一个的递归构造，娴熟地运用了有限域理论、代数数论、正交拉丁方和横截设计 (transversal design), “横截系列” (即 “T-系列” 的概念是1961年哈那尼引入的^[45]) 等工具和成果，通过前后16个引理、29个定理给出了以下五个各具特色的递归结果，可归纳为^[21]：

$$\text{I. } d(v+2) = v \xrightarrow[v \notin T]{v \equiv 11 \pmod{12}}$$

$$d(3v) = 3v - 2,$$

$$(T = \{23, 47, 59, 83, 107, 167, 179, 227, 263, 299, 347, 383, 719, 767, 923, 439\})$$

$$\text{II. } d(v+2) = v \xrightarrow[\text{或 } p=5, 17, 19, 29]{\text{素数 } p \equiv 7 \pmod{8}}$$

$$d(pv+2) = pv; \quad (p=5 \text{ 时}, v \neq 1)$$

$$\text{III. } d(2v+1) = 2v - 1$$

$$\text{存在12个 } v \text{ 阶正交拉丁方} \xrightarrow{v \text{ 奇}}$$

$$d(12v+1) = 12v - 1;$$

$$\text{IV. } d(4v+1) = 4v - 1 \xrightarrow[p=1, 2, 5]{} \longrightarrow d(12pv+1) = 12pv - 1;$$

$$\text{V. } d(4v+1) = 4v - 1 \xrightarrow[v \text{ 奇}]{p=7, 11}$$

$$d(12pv+1) = 12pv - 1.$$

在第六篇论文中，陆家羲按照以下的格局进行了分析^[21]：

并分别应用上述 I ~ V 以及以上所说的特林克和罗沙的两个递归结果，最终得到了大集定理。至此，历时一百三十余年的不相交斯坦纳三连系大集问题已宣告解决。

至于该定理所遗留的六个整数值 $141, 283 (= 141 \times 2 + 1)$, $501, 789, 1501 (= 501 \times 3 - 2)$, $2365 (789 \times 3 - 2)$ 的大集是否存在，1983年5月30日陆家羲在介绍他自己的工作时写道：“我正准备写论文 VII，以除去六个可能的例外。”^[46]1983年7月30日在大连全国组合数学首届学术会议全体会上，陆家羲宣布业已找到这六个值的大集构造方法，即将成文。然而令人不胜痛惜的是，他在长期艰苦条件下孤军奋战，终于积劳成疾，心力交瘁，不幸于1983年10月31日凌晨猝然辞世，中断了他的工作和学者们对他更高的期望。

在陆的遗稿中人们找到了“互不相交的 Steiner 三元组系列的最大集 VII”24页提纲，记录了他攀登大集定理这个数学高峰如何跨出最后一步的设想……死神在最后一瞬间带走了他，似乎是要把这最后的秘密一同带到另一个世界。

……时间过去了五年，尽管国内外学者尽了很大努力，尽管一部分学者还掌握那24页提纲，尽管有人还用计算机作为辅助工具，但在笔者写到这里的时候，还没有听到关于那六个值（哪怕是最小的一个）的大集已完全构造成功的消息。*

我们相信这一遗憾将不会是永恒的，并殷切

地寄希望于来者，描完陆家羲的大集定理未竟的最后一笔。

正象康庆德教授所说：“尽管有此遗憾，他二十多年含辛茹苦、呕心沥血所获得的这一成果仍是组合设计领域中这一世界性难题的最卓越的答案。在这方面他占有着无可争议的领先权。作为一名地处边陲的普通中学的物理教师，面对困窘的科研、生活条件 and 一再的挫折、打击、非难，他怀着一颗为祖国争光、为民族争气的雄心，在出色地完成繁重教学任务的同时，奋力拚搏，冲击世界高峰，终于一举登上了这一峰峦，在科学的史册上为我中华又增书了光辉的一页。”^{〔21〕}

1984年9月，内蒙古自治区科委和数学会邀集国内组合数学界专家、学者组织了“陆家羲学术工作评审委员会”，“会议以小组讨论为主，充分地认真地研究了大会发言，特别是康庆德、吴利生二同志发言中提出的几个需要进一步研究落实的问题。经过努力，提出的全部疑点都得到排除。9月15日，大会一致认定陆家羲的论文《On Large sets of disjoint Steiner triple systems I—VI》中宣布的除 $v \in \{141, 283, 501, 789, 1501, 2365\}$ 待进一步研究外，当 $v \equiv 1, 3 \pmod{6}$ ， $v > 7$ 时， $d(v) = v - 2$ 这一科学结论，是正确无误的。一致认为，陆家羲同志的这一学术成就是卓越的，可与二十年前欧拉猜测的否定

(1959, 1960) 和 $k = 3, 4$ 时 (b, v, r, k, λ) -设计存在的充要条件的证明 (1961) 这两项卓越成就相媲美。陆家羲以一个业余的数学工作者，潜心钻研数学二十余年，在一个难度极大并具有重大学术价值的问题上，解决了百余年来全世界许多组合学家曾致力但未能解决的问题，为国家争得了荣誉，为后人树立了刻苦努力的楷模。与会同志一致认为对于这样一位优秀的科学家应给予适当的精神和物质奖励。认为，给予陆家羲同志以国家一或二等自然科学奖是适宜的。”

“这次会议受到内蒙古自治区领导的高度重视。……自治区新闻界也给予了积极的关注和支持。”

“会议对内蒙古数学学会提出以下建议：

1. 吁请国内专家，努力设法尽快把陆家羲同志来不及完成的论文Ⅶ的证明加以补证，使结论达到圆满无缺的地步；

2. 设法出版陆家羲论文专集；

3. 清理陆家羲同志关于科克曼问题的遗作，弄清此一问题解决的学术优先权。”（摘自陆家羲学术工作评审会议纪要）

继包头市政府给予陆家羲以奖励之后，1984年10月31日中共内蒙古自治区委员会、内蒙古自治区人民政府颁发了“关于向优秀知识分子陆家羲同志学习暨表彰的决定”，授予他科技进步特等奖，并在包头召开了表彰大会。

为了进一步认识大集定理, 以下应用陆家羲论文中给出的一种方法来构造一个37阶的斯坦纳三元系大集, 这是该文发表前尚未给出答案的最小的一个 v 值, 所用到的方法也是该文一系列构造法中最简单的一种^[21]。

由于 $d(37) = 35$, 即有35个互不相交的 $S(37)$ 构成此大集, 共有 $\binom{37}{3} = 7770$ 个互不相同的三元组, 每个 $S(37)$ 有222个区组。怎样来表达这样一个庞大的(对组合数学家说来却是很小的)结构都是一件费脑子的事。为了避免过多的符号, 缩小篇幅, 加强直观, 康庆德教授对记法作了一些改变, 并不加证明地直接给出在集合 $X = \{0, 1, \dots, 36\}$ 上的 $S(37)$ 大集。用 Z_n 表示整数集 Z 的模 n 剩余类集合, 它的元素一般记为 $\{0, 1, \dots, n-1\}$ 。构造的途径是:

由集合 $\{a, b\} \cup Z_7$ 上的9阶三连系大集与集合 $\{a, b\} \cup Z_5$ 上的 $5 \times 7 = 35$ 个(对每个区组分别规定了顺序及参数的) $S(7)$, 进行指定的“并合”, 最终得到集合 $\{a, b\} \cup (Z_7 \times Z_5)$ 上的 $d(37) = 35$ 个两两不相交的 $S(37)$ 。

下文中的 (L_1) 、 (L_2) 、 (L_3) 和 (L_4) 为陆家羲给出的区组分类。对 $i \in Z_5, k \in Z_7$ 的每对 i, k 值, 这些区组的全体即构成一个 $S(37)$ 。其中 (L_1) 给出12个区组, (L_2) 给出84个区组, (L_3) 给出28个区组, (L_4) 给出98个区组, 总计对每个 $S(37)$ 给

出 $(37 \times 36)/6 = 222$ 个区组。记法中 $[x]$ 和 $\langle x \rangle$ 分别表示 x 对模 7 和模 5 取值, 变数 u, v (除 (L_i) 中指出的限制外) 均独立地遍取 Z_7 中的值, 变数 i, k 是用以区分不同三连系的, 而 $j = 1, 2$ 。诸参数 $\alpha_{kj}, \beta_{kj}, \phi_{kj}, \gamma_{kj}, \delta_{kj}, \psi_{kj}, \lambda_{kj}, \mu_{kj}, \chi_{kj}$ 的取值如下表:

k	j	α_{kj}	β_{kj}	ϕ_{kj}	γ_{kj}	δ_{kj}	ψ_{kj}	λ_{kj}	μ_{kj}	χ_{kj}
0	1	3	4	2	1	3	1	1	4	0
	2	2	1	0	4	2	2	3	2	0
1	1	4	3	-1	1	4	-2	1	3	1
	2	2	1	1	3	2	2	4	2	-1
2	1	2	4	2	4	1	-1	3	4	2
	2	1	3	-2	3	2	-2	2	1	-2
3	1	3	4	-3	1	3	3	1	4	3
	2	2	1	-3	4	2	-3	3	2	3
4	1	1	3	4	3	4	-4	1	4	4
	2	4	2	4	2	1	-4	3	2	4
5	1	4	1	0	3	4	1	1	3	2
	2	2	3	-2	1	2	-1	4	2	-2
6	1	4	2	1	1	4	0	3	4	1
	2	3	1	-1	2	3	0	2	1	-1

$(L_i): \{7i + [k], 7i + [1 + k], 7i + [6 + k]\},$
 $\{7i + [k], 7i + [2 + k], 7i + [5 + k]\},$
 $\{7i + [k], 7i + [3 + k], 7i + [4 + k]\},$
 $\{7i + [1 + k], 7i + [2 + k],$
 $7i + [4 + k]\},$
 $\{7i + [3 + k], 7i + [5 + k],$
 $7i + [6 + k]\},$

$$\begin{aligned}
& \{35, 7i + [4 + k], 7i + [6 + k]\}, \\
& \{35, 7i + [2 + k], 7i + [3 + k]\}, \\
& \{35, 7i + [1 + k], 7i + [5 + k]\}, \\
& \{36, 7i + [6 + k], 7i + [2 + k]\}, \\
& \{36, 7i + [3 + k], 7i + [1 + k]\}, \\
& \{36, 7i + [5 + k], 7i + [4 + k]\}, \\
& \{35, 36, 7i + [k]\};
\end{aligned}$$

$$\begin{aligned}
(L_2): & \{7\langle\alpha_{kj} + i\rangle + [2(\phi_{kj} + v) - u], \\
& 7\langle\alpha_{kj} + i\rangle + u, 7\langle\beta_{kj} + i\rangle + v\}, \\
& \{7\langle\gamma_{kj} + i\rangle + [2(\psi_{kj} + v) - u], \\
& 7\langle\gamma_{kj} + i\rangle + u, 7\langle\delta_{kj} + i\rangle + v\} \\
& \text{(上组中 } u \neq [\phi_{kj} + v], \text{ 下组中 } u \neq \\
& [\psi_{kj} + v]);
\end{aligned}$$

$$\begin{aligned}
(L_3): & \{35, 7\langle\alpha_{kj} + i\rangle + [u + \phi_{kj}], \\
& 7\langle\beta_{kj} + i\rangle + u\}, \\
& \{36, 7\langle\gamma_{kj} + i\rangle + [u + \psi_{kj}], \\
& 7\langle\delta_{kj} + i\rangle + u\};
\end{aligned}$$

$$\begin{aligned}
(L_4): & \{7i + u, 7\langle\lambda_{kj} + i\rangle + v, \\
& 7\langle\mu_{kj} + i\rangle + [\chi_{kj} - u - v]\}.
\end{aligned}$$

在本书已近完成时，得到中央人民广播电台、中央电视台播出的新消息：陆家羲对不相交斯坦纳三元系大集的研究，已获得1987年国家自然科学一等奖^[70]。这是我国对自然科学和技术创造性成果的最高奖励。

“在获奖成果中，有不少是长期研究工作的积累，许多科学家为此付出了毕生精力。有28位

同志已经去世，他们为祖国的科学事业作出了杰出贡献。”是的，陆家羲老师为祖国的科学和教育事业鞠躬尽瘁，死而后已，创造了具有世界水平的科学成果，他获得这样崇高的荣誉，是当之无愧的，是理所当然的。

陆家羲去世后，在国内组合学界、数学界、教育界、舆论界乃至社会上产生了巨大的反响，国外学者也来信、来电表示哀悼。这方面的大量信息，可以参考文献^[77]，以及以后报章杂志发表的回忆、报导、报告文学等。

本世纪30年代，英国人应用正交设计编制农田小麦实验方案取得成功，区组设计的实际应用背景又一次得到证明^[78]。当代著名统计学家费希尔^[79]把斯坦纳系问题与统计学的实验设计与分析联系起来，大大促进了它的发展。在现代的研究中，区组设计对数字通讯、快速变换、有限几何等应用和理论学科业已显示出重要的作用。

斯坦纳三连系的一个应用可能出现在检验 v 种产品的质量上，如果每两种产品都要进行比较，而每次检验只能有效地区别三种产品。另外，科克曼三连系将给出一个有意义的方案，在其中每个产品恰好每天使用一次^[13]。我们还可将这些方案应用于体育训练中，或者再增加一些条件，使 V 个用人单位对 v 个毕业生的三项要求，与 v 个毕业生对 V 个用人单位的三项希望恰能互适。在分配方案方面的工作，似乎还有未加开发的前

景。至于不相交斯坦纳三连系，1965年多耶勒特著文^[40]，认为这种构造可以用于某些统计实验的设计。

60年代以来，由于计算机科学的崛起，在广泛的实际应用背景的刺激下，组合数学的发展已进入一个新的历史时期。以《组合论杂志》的创立（1966）为标志，在国际上兴起了研究的新高潮，是史无前例的：出版了一批组合论专著，以莱塞^[11]和霍尔^[45]的书影响较大，并开始译成多种文字，它们全面介绍组合理论，对区组设计和斯坦纳系亦辟有专门的章节；发行了一批论文集、会议文集，出版了一批大学教材。现在，离散数学、组合数学、图论等已成为许多大学计算机系、数学系必修或选修课了。

根据组合学家多延和罗沙所编斯坦纳系文献一览^[11]，1960年到1982年10月发表757篇（其中50篇待发），占1844年—1982年10月有关论文总数的81%，反映了现代发展的强大势头。各国出现了一大批组合学家，仅在斯坦纳系方向上有著述的就达410人之多，其中大部分是现代学者，近20人有10篇以上论文发表（包括与人合作）。以最初发表这方面论文先后为序，他们是：

斯坦顿1951—1981年13篇，霍尔1954—1967年15篇，哈那尼1960—1977年13篇，罗沙1963—1982年38篇，阿斯穆斯1966—1981年12篇，多延1969—1981年18篇，穆林1969—1982年11篇，

N.S. 曼德尔逊1969—1978年13篇，林德奈1971—1981年49篇，米尔斯1972—1981年12(待发1)篇，德尼斯顿1972—1980年16(待发1)篇，威尔逊1972—1974年13篇，特林克1973—1979年13(待发1)篇，克雷莫1974—1980年11篇，费尔普斯1975—1981年25(待发1)篇，哈特曼1978—1982年13(待发2)篇，科尔本1980—1982年22(待发10)篇。

这反映了现代研究的一个侧面。可以看出，许多著名组合学家也正是60年代以来才展开他们的工作的。我国以陆家羲为代表的一批中青年组合学工作者已经克服了重重困难，在区组设计的领域内崭露头角。同时，也应清醒估计到，国外的研究，已有多年积累的雄厚基础；在一个较长时期内，吸收国外先进成果开创新的局面仍然是艰巨的任务。1988年8月在安徽屯溪召开了区组设计国际会议，1990年8月在安徽合肥将召开国际组合数学暨第四届中国组合数学学术会议，将带来近年研究的最新信息。

由于斯坦纳系在上世纪末就已形成了一个数学研究的专题，本世纪初就有人搞“科克曼女生问题索引”^[82]和撰与有关详细历史^[83]。由于文献剧增，出现介绍进展的文章“斯坦纳三连系的新近结果”^{[84][85]}。除上述文献^[81]外，还有“斯坦纳系文献一览”^[86]。这些材料，对从事于这方

面工作的专业人员和有志于此道的青年学者十分有用。

*根据最新得到的信息，荷兰学者L. Teirl-nch已于1989年10月解决了这一问题。他基本是从LD设计入手取得了突破的。

十二、关于Nim 型对策和 Nim 三连系



在本书开始所叙述的 Chinese game of Nim 大体上还是 Nim 作为游戏的历史。近百年来，由于数学家的介入，Nim 成了斗法的战场。我们已经看到，Nim 制胜方案可以看作一种斯坦纳三连系，一种科克曼三连系。然而事情还不止此，随着数论、近世代数、逻辑代数、特别是对策论、图论和组合数学的发展，当人们用新的眼光观察 Nim 时，它作为一种数学模型，又给人以新的启示，引起了广泛的兴趣。于是 Nim 升格了，不再仅仅是一种游戏，一跃而成为一个新的数学名词，开始在数学论文和专著中出现。

我们先来看破解 Nim 的方法，以抓三堆为例。将三堆石子的数目用二进制数表示出来，例如11，22，29：

$$\begin{array}{r} (11)_{10} = (1011)_2 \\ (22)_{10} = (10110)_2 \\ (29)_{10} = (11101)_2 \\ \hline \end{array}$$

$$00000$$

上式中所进行的运算是一种特殊的加法，即 1 加 1 为 0，1 加 0 为 1，0 加 0 仍为 0。如果一个人抓三堆时面临三堆的数字如上式一样其和为 0，那么无论他按照规则取出多少，只要对方以后步步不错，等待他的必然是失败。这种加法在数学上叫“点加”或“模 2 加”，加出来的和叫“点和”或“布尔和”。如果点和不为 0，该谁取，谁便交了好运，唯一正确的取法会使他把点和为 0 的局面留给对手，这将保证他取胜。同样的原则也适用于堆数更多的情况。将布尔和为 0 的三元组记录下来，就得到表 1 的结果，于是我们便发现了图论中 Nim 型对策与组合数学中的斯坦纳系的联系。

在图论中，Nim 似乎受到了特别的重视。法国数学家贝尔热在 1962 年出版的一本颇有影响的专著《图论及其应用》⁽²⁾ 中专门开辟了一章（第六章）来介绍“在一个图上的对策”，主要是研究“Nim 型对策”。这里的“对策”，指的就是游戏或博弈(game)。贝尔热在书中说，为了纪念这个人们熟悉的游戏，在数学上定义的、广义的 Nim，便命名为“Nim 型对策”。

首先，图论学者把一局 Nim 中可能出现的各种局面与一个图的各个顶点联系起来。这里所指的图，是由若干个顶点与连接其中某些顶点的有向边所组成的图形，并且要求每两个顶点之间至多只能有一条有向边相连（即所谓 1-图）。把

一个图的顶点集合 $\{x_0, x_1, \dots, x_n\}$ 记为 X 。若对于 $x_i, x_j \in X$, x_i 与 x_j 之间有一条有向边相连, x_i 为起点, x_j 为终点, 则称 x_j 为 x_i 的后继顶点。对于某个 $x_i \in X$, x_i 的所有后继顶点的集合记为 $\Gamma(x_i)$ 。于是, Nim 型对策的定义就可以表示为²⁾:

给定一个图, 并且任意选定图的一个顶点 x_0 作为初始顶点。两位选手 A 、 B 交替进行: 选手 A 首先从集合 $\Gamma(x_0)$ 中选择一个顶点 x_1 , 选手 B 接着从集合 $\Gamma(x_1)$ 中选择一个顶点 x_2 , 如此等等。如果一个选手所选顶点 x_k 使得 $\Gamma(x_k) = \phi$ (空集), 那么游戏就结束了。胜家就是这个选择最后顶点的选手。当然, 这个图不能有由首尾相接的有向边所组成的圈, 不然游戏就有可能无限进行下去。

例如, 在抓三堆 Nim 中, 我们使每个局面 $\{a, b, c\}$ 对应于空间笛卡儿坐标系下的非负整数格点 (a, b, c) , 把这些格点作为图的顶点。若两个顶点 $\{a, b, c\}$ 与 $\{a', b', c'\}$ 满足下列条件之一:

- (i) $a > a', b = b', c = c'$,
- (ii) $a = a', b > b', c = c'$,
- (iii) $a = a', b = b', c > c'$,

就定义 $\{a', b', c'\}$ 是 $\{a, b, c\}$ 的后继顶点, 即存在一条以 $\{a, b, c\}$ 为始点、以 $\{a', b', c'\}$ 为终点的有向边。这样, 抓三堆 Nim 就成为上述 Nim 型对策的一个特殊例子了。

由此可见, Nim 型对策的图论意义在本质上揭示了 Nim 的特性, 从而扩大了 Nim 的外延, 使得原来从形式上看似乎与 Nim 无缘的一些图的游戏、扑克游戏、数字游戏等都归于这一类。例如霍普金斯大学的伊萨克斯发明的游戏, 即所谓“围棋盘上下国际象棋”¹⁾, 成了典型的 Nim。又如“斐波那契 Nim”, 只用一堆火柴, 规定每人所取火柴数目不得超过前一次对手所取数目的二倍, 最后谁取完谁胜。诸如此类的新花样可以任人设计, 层出不穷。从这个意义上讲, Nim 在对策论、图论中又复兴了。

在《图论及其应用》一书中, 为了刻画 Nim 制胜局面的特性而把主要结果表述成四个定理。这里只看定理 1:

假如一个图拥有一个核 S , 并且假定一个选手选择了核 S 中的一个顶点, 那么这一选择将保证他取胜或得平局。

所谓图的一个核 S 是顶点集合 X 的一个子集, 它满足 (i) 若 $x \in S$, 则 $\Gamma(x) \cap S = \emptyset$; (ii) 若 $x \notin S$, 则 $\Gamma(x) \cap S \neq \emptyset$ 。

现在来证明这个定理。由核的定义, 容易知道, 假如选手 A 选 $x_1 \in S$ 使得 $\Gamma(x_1) = \emptyset$, 此时他显然为胜家; 否则他的对手 B 将被迫在 $X \setminus S$ 中选择一个顶点 x_2 。然后, 选手 A 在下一轮中又能在核 S 中选择一个顶点 x_3 , 如此等等。当一位选手选择一个顶点 x_k , 使得 $\Gamma(x_k) = \emptyset$ 时,

必然 $x_k \in S$, 游戏于是到此结束。由于选手 B 不可能在 S 中选择, 因此, 若过程有限, 则选手 A 为胜家, 若过程无限, 则获平局。

该书在以后的三个定理中应用了 “Grundy 函数” (或称 “Sprague-Grundy 函数”) 的概念, 它是顶点集合 X 到非负整数集合内的一个映射 $g(x)$ 。对于每一个顶点 $x \in X$, Grundy 函数 $g(x)$ 被定义为在 x 的所有后继顶点 x' 的 Grundy 函数值集合 $\{g(x')\}$ 中不出现的最小非负整数。特别地, 假如 $\Gamma(x) = \phi$, 那么 $g(x) = 0$ 。Grundy 函数是研究 Nim 而引入的, 它的定义体现了一种递归关系, 确保这种关系的延续与确保最终的胜利具有同样的意义。因而用它轻易解决了三种类型的 Nim。不仅如此, Grundy 函数对于所有组合对策都是重要的。只要图中没有圈, 那么就存在这个图的唯一的 Grundy 函数。可以证明, 一个图若有 Grundy 函数 $g(x)$, 则这个图一定有一个核 S , 这个核就是 $\{x | g(x) = 0\}$ 。

对于抓三堆 Nim, Grundy 函数可以定义为三堆数目的点积。引前边的例子知 $g(\{11, 22, 29\}) = 0$, 因此它是一个制胜局面。三元组 $\{11, 22, 29\}$ 所表示的顶点 $x \in S$, 换言之, 上述表 1 恰恰构成了抓三堆 Nim 的核 S 。科克曼在历史上给出的第一个可分解平衡不完全区组设计方案, 即十五个女生问题的解也恰恰是这样的一个

核 S , 大概不是一个偶然的事件。

以下, 我们将引入“Nim三连系”的概念。

对于一个正整数 a , 它可以表示为

$$a = 2^{a_1} + 2^{a_2} + \dots + 2^{a_n} \quad (12.1)$$

这里 $a_i (i=1, 2, \dots, n)$ 是非负整数 与 a 对应的有集合 A

$$A = \{2^{a_1}, 2^{a_2}, \dots, 2^{a_n}\} \quad (12.2)$$

对每个正整数都作这样的对应, 再补充定义 0 对应 ϕ (空集), 于是构成了从非负整数集合到由 2 的幂组成的集合上的一个映射 φ , 显然 φ 是一一映射。

在定义 Nim 三元组之前, 引用集合论中的对称差的概念 (陆家羲在解决科克曼女生问题以及 BIB 问题时曾应用过它), 这里作较详细的介绍。非空集合 A 与 B 的对称差 (symmetrical difference, СИММЕТРИЧЕСКАЯ РАЗНОСТЬ) 记作 $A \Delta B$, 定义⁽⁸⁷⁾⁽⁸⁸⁾

$$\left. \begin{aligned} A \Delta B &= \{x | x \in A, x \in B, x \notin A \cap B\} \\ A \Delta B &= (A \cup B) \setminus (A \cap B) \\ A \Delta B &= (A \setminus B) \cup (B \setminus A) \\ A \Delta B &= (A \cap \bar{B}) \cup (\bar{A} \cap B) \end{aligned} \right\} \quad (12.3)$$

另外, 当 E 为全集而 $A \cup B = E$ 的条件下有

$$A \Delta B \stackrel{*}{=} \bar{B} \cup \bar{A} \quad (* \text{ 号表示成立的条$$

件)。对称差满足交换律、结合律、交的分配律。

引。如果 $A \Delta B = C$, 那么 $A \Delta C = B, B \Delta C$

$= A$ 。

证明： $B \triangle C = B \triangle (A \triangle B) = B \triangle (B \triangle A)$

$$= (B \triangle B) \triangle A = A.$$

$$A \triangle C = A \triangle (A \triangle B) = (A \triangle A) \triangle B$$

$$= B.$$

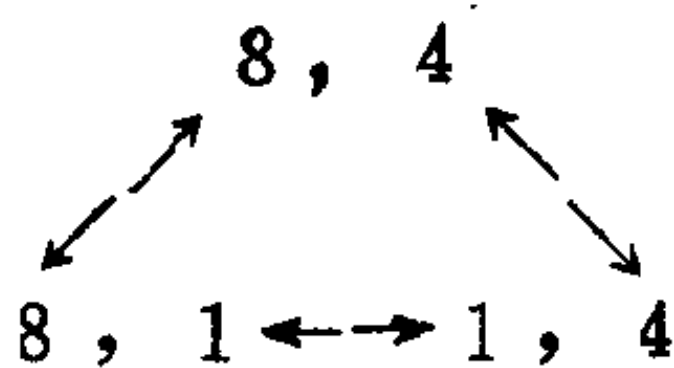
定义：如果 $A \triangle B \triangle C = \phi$ ，那么在映射 φ 下的三个正整数 a, b, c 叫做一个 Nim 三元组。

例. 12, 9, 5 构成一个 Nim 三元组，在映射 φ 下的三个集为 A, B, C ，由 (12.1) 和 (12.2) 知

$$a = 12, A = \{4, 8\}$$

$$b = 9, B = \{1, 8\}$$

$$c = 5, C = \{1, 4\}$$



于是 $A \triangle B \triangle C = \{4, 8\} \triangle \{1, 8\} \triangle C = \{1, 4\} \triangle \{1, 4\} = \phi$ 。

Nim 三元组具有几个有趣的性质：

性质1. 若 $\{a, b, c\}$ 是 Nim 三元组，则在 φ 下 A, B, C 每一个都是另两个的对称差集。

证明： $A \triangle B \triangle C = \phi \implies (A \triangle B) \triangle C = C \triangle C \implies A \triangle B = C$ 。同理可证： $A = B \triangle C, B = A \triangle C$ 。

系1：两个不相等的正整数确定唯一的 Nim 三元组。

系2：Nim 三元组个数无限多。

性质2. Nim 三元组中一元不大于另外两元之和，不小于另外两元之差。

证明: $\{a, b, c\}$ 是 Nim 三元组, 考虑 $b > c$, 在 φ 下设 $B \cup C = E$, $B \cap C = F$, 当 $F = \phi$ 时 $f = 0$; $B \setminus F = \bar{C}$, $C \setminus F = \bar{B}$; 当 $\bar{B} = \phi$ 时 $\bar{b} = 0$.

(i) $A \Delta B \Delta C = \phi \implies A = B \Delta C = (B \cup C) \setminus (B \cap C) = E \setminus F$; $E \supset F$, $A = E \setminus F \implies a = e - f$;
 $B \cup \bar{B} = E$, $B \cap \bar{B} = \phi \implies b + \bar{b} = e$; $C = \bar{B} \cup F$,
 $\bar{B} \cap F = \phi \implies c = \bar{b} + f$; $b + c = b + (\bar{b} + f) = (b + \bar{b}) + f = e + f$. $\therefore a = e - f \leq e + f = b + c$. (不等式当且仅当 $f = 0$ 即 $B \cap C = \phi$ 时取等号)。

(ii) $A \Delta B \Delta C = \phi \implies A = B \Delta C = (B \cap \bar{C}) \cup (C \cap \bar{B}) = \bar{C} \cup \bar{B}$, $\bar{C} \cap \bar{B} = \phi \implies a = \bar{c} + b$. 又 $b > c$.

$$\left. \begin{aligned} B &= \bar{C} \cup F, \bar{C} \cap F = \phi \implies b = \bar{c} + f \\ C &= \bar{B} \cup F, \bar{B} \cap F = \phi \implies c = \bar{b} + f \end{aligned} \right\} \implies b - c = \bar{c} - \bar{b},$$

$\therefore a = \bar{c} + \bar{b} \geq \bar{c} - \bar{b} = b - c$ (不等式当且仅当 $\bar{b} = 0$ 即 $C \subset B$ 取等号)。

对 a 所作结论, 对 b 或 c 也成立。证完。

易于联想到, 许多 Nim 三元组 ($f \neq 0$, $\bar{b} \neq 0$) 中的三元 a, b, c 可以作为边长交成三角形, 不妨称为 Nim 三角形。

性质 3. 设 $\{a, b, c\}$ 为 Nim 三元组, σ 为正整数, 那么 $2^{\sigma-1} \leq a < 2^\sigma \implies b < 2^\sigma$, $c < 2^\sigma$ 或 $b \geq 2^\sigma, c \geq 2^\sigma$ 。

证明: I. 当 $a > b > c$ (或 $a > c > b$) 时, 显

然 $b, c < 2^\sigma$; I. 当 $b > a > c$ (或 $c > a > b$) 时,
 (i) 当 $2^\sigma > b$, 显然 $b, c < 2^\sigma$; (ii) 当 $2^\sigma \leq b$, 这
 时 $c < a$, 不可能; II. 当 $b > c > a$ 或 $c > b > a$,
 在 φ 下, (i) 当 $b = 2^\sigma, a < 2^\sigma \Rightarrow 2^\sigma \notin A, 2^\sigma \in B$
 $\Rightarrow 2^\sigma \in B \cap \bar{A} \Rightarrow 2^\sigma \in (B \cap \bar{A}) \cup (\bar{B} \cap A) \Rightarrow$
 $2^\sigma \in A \Delta B = C \Rightarrow 2^\sigma \leq C$, 又 $b \neq c \Rightarrow c > 2^\sigma$, 同
 理, 当 $c = 2^\sigma \Rightarrow b > 2^\sigma$, (ii) 当 $b > 2^\sigma, a < 2^\sigma \Rightarrow$
 必有 $2^{\beta_j} \geq 2^\sigma$ 使 $2^{\beta_j} \in B$ 而 $2^{\beta_j} \notin A \Rightarrow 2^{\beta_j} \in B \cap$
 $\bar{A} \Rightarrow 2^{\beta_j} \in (B \cap \bar{A}) \cup (\bar{B} \cap A) \Rightarrow 2^\sigma \in A \Delta B =$
 $C \Rightarrow 2^{\beta_j} \leq c \Rightarrow c \geq 2^{\beta_j} \geq 2^\sigma$. 同理, 当 $c > 2^\sigma \Rightarrow$
 $b \geq 2^\sigma$.

对 a 所作结论, 对 b 或 c 也成立。证完。

性质 4. 设 a, b, c 为三个正整数, 如果
 $2^{\sigma-1} \leq a < 2^\sigma$, 令 $b' = 2^\sigma t + b, c' = 2^\sigma t + c$, 其中
 t 为正整数, 则 $\{a, b', c'\}$ 为 Nim 三元组的充要
 条件是 $\{a, b, c\}$ 为 Nim 三元组。

分析: 根据性质 3, $b, c < 2^\sigma$ 或 $b, c \geq 2^\sigma$. 前

者在映射 φ 下, 设 $T = \{x \mid x = 2^{\tau_i}, \sum_{i=0}^m 2^{\tau_i} = t,$

$0 \leq \tau_i, m \leq \log_2 t\}, J = \{x \mid x = 2^{\sigma+\tau_i}, \sum_{i=0}^m 2^{\sigma+\tau_i} = 2^\sigma t,$

$0 \leq \tau_i, m \leq \log_2 t\}$, 有 $t \longleftrightarrow T, 2^\sigma t \longleftrightarrow J$. 由
 $2^{\beta_j} \in B, \sum 2^{\beta_j} = b < 2^\sigma \Rightarrow 2^{\beta_j} < 2^\sigma$, 又 $2^{\sigma+\tau_i} \in J \Rightarrow$
 $2^{\beta_j} \notin J, 2^{\sigma+\tau_i} \notin B \Rightarrow J \cap B = \phi$. 同理 $J \cap C = \phi$.

$B' = J \cup B, B = B' \setminus J = B' \cap \bar{J}; C' = J \cup C, C = C' \setminus$

$$\begin{aligned}
 J &= C' \cap \bar{J}, \quad B' \cap C' = (J \cup B) \cup (J \cup C) = J \cup (B \cup C); \\
 B' \cup C' &= (J \cup B) \cap (J \cup C) = J \cup (B \cap C), \\
 B \cup C &= (B' \cup \bar{J}) \cup (C' \cap \bar{J}) = (B' \cup C') \cap \bar{J}, \\
 B \cap C &= (B' \cap \bar{J}) \cap (C' \cap \bar{J}) = (B' \cap C') \cap \bar{J}.
 \end{aligned}$$

以下的证明只给出 $b, c < 2^s$ 时的情况。

证明: (i) 由 $\{a, b, c\}$ 是 Nim 三元组 $\Rightarrow A \triangle B \triangle C = \phi \Rightarrow A = B \triangle C = (B \cup C) \setminus (B \cap C) = [(B' \cup C') \cap \bar{J}] \cap [(B' \cap C') \cap \bar{J}] = [(B' \cup C') \cap \bar{J}] \cap [(B' \cap C') \cap \bar{J}] = (B' \cup C') \cap \{[\bar{J} \cap (\bar{B}' \cup \bar{C}')] \cup J\} = (B' \cup C') \cap \{[\bar{J} \cap (\bar{B}' \cup \bar{C}')] \cup (\bar{J} \cap J)\} = (B' \cup C') \setminus J \cup (B' \cap C') = (B' \cup C') \setminus (B' \cap C') = B' \triangle C' \Rightarrow A \triangle B' \triangle C' = \phi \Rightarrow \{a, b', c'\}$ 是 Nim 三元组。

(ii) 由 $\{a, b', c'\}$ 是 Nim 三元组 $\Rightarrow A \triangle B' \triangle C' = \phi \Rightarrow A = B' \triangle C' = (B' \cup C') \setminus (B' \cap C') = [J \cup (B \cup C)] \cap [\bar{J} \cup (\bar{B} \cap \bar{C})] = [J \cup (B \cup C)] \cap [\bar{J} \cap (\bar{B} \cup \bar{C})] = \{(J \cap \bar{J}) \cup [(B \cup C) \cap \bar{J}]\} \cap (\bar{B} \cup \bar{C}) = (B \cup C) \cap (\bar{B} \cup \bar{C}) = \bar{B} \cup \bar{C} = B \triangle C \Rightarrow A \triangle B \triangle C = \phi \Rightarrow \{a, b, c\}$ 是 Nim 三元组。

在 $b, c \geq 2^s$ 时也可证得同样的结果。对于 a 的结论对 b 或 c 也成立。证完。

根据性质 4 以及它的特殊情况—— $\{a, 2^s t, 2^s t + a\}$ 是一个 Nim 三元组, 我们可以从一个最简单的 Nim 三元组 $\{1, 2, 3\}$ 推出任何一个 Nim 三元组来 (下例给出求 $\{15, 17, 30\}$ 的过程), 亦即可用演绎的方法给出 Nim 制胜方案。

例. 由 Nim 三元组 $\{1, 2, 3\}$ 推知 $\{1, 2t,$

$2t+1\}$ 是一个 Nim 三元组, 取 $t=7$, 得 $\{1, 14, 15\}$, 推知 $\{15, 16t+1, 16t+14\}$ 也是一个Nim三元组, 取 $t=1$ 得 $\{15, 17, 30\}$ 。

我们把 $\{1, 2, 3\}$ 和 $\{a, 2^{\sigma}t, 2^{\sigma}t+a\}$ 看作边界条件, 应用性质 4, 可以得到一系列的 Nim 三元组的通项公式:

$$\{1, 2t, 2t+1\}, \{2, 4t+1, 4t+3\},$$

$$\{3, 4t+1, 4t+2\},$$

$$\{2, 4t, 4t+2\}, \{3, 4t, 4t+3\}, \dots$$

取 t 过自然数, 到某个需要的 (或足够大的) n 为止, 再对所得各三元组应用上法, 即复制出全部所需三元组族——Nim 三连系。我们在节一中所给出 Nim 制胜方案的通项公式已包含其中, 这一构造的正确性同时得到证明。

在有限个Nim三元组中必有最大元 a_{\max} (最大的正整数):

$$2^{n-1}-1 < a_{\max} \leq 2^n-1 = v \quad (n \geq 2)$$

定义: 最大元是 v 的 Nim 三元组的全集称为 v 阶 Nim 三连系, 记作 $\text{NTS}(v)$ 或 $\text{NTS}(2^n-1)$ 。

例。表 6 是一个 7 阶Nim三连系 $\text{NTS}(7)$; 表 1 横线以下的部分和表 2 各是一个15阶Nim三连系 $\text{NTS}(15)$ 。

显然, $\text{NTS}(v)$ 是一个 v 阶斯坦纳三连系。我们有:

性质 5. (i) $\text{NTS}(v)$ 所有三元组中共有 $v =$

$2^n - 1$ 个不同的元, 即 $1, 2, \dots, 2^n - 1$ 。

(ii) $\text{NTS}(v)$ 中任意两元只出现于其中一个三元组。

(iii) $\text{NTS}(v)$ 中共有三元组数 $b = v(v - 1)/6$ 。

证明: 由 (i) 知, $\text{NTS}(v)$ 中共有 $v = 2^n - 1$ 个不同元, 所有元可以构成无重复的二元组共 $\binom{2^n - 1}{2}$ 个; 每个三元组中容有三个不同的二元组。据 (ii) 可知, Nim 三连系中共有三元组数: $b = \frac{1}{3} \binom{2^n - 1}{2} = v(v - 1)/6$ 。

(iv) $\text{NTS}(v)$ 中每一元重复出现的次数 $r = (v - 1)/2$ 。

证明: $\text{NTS}(v)$ 中包括重复元在内的总元数为 $3b = v(v - 1)/2$, 每一元重复出现的次数 $r = 3b/v = (v - 1)/2$ 。

系 1. $\text{NTS}(2^n - 1) \subset \text{NTS}(2^{n+1} - 1)$ 。

系 2. v 阶 Nim 三连系是一个 v 阶 Steiner 三连系。

引理. $2^n - 1$ 必具 $6m + 1$ 或 $6m + 3$ 之形 (n, m 为非负整数)。

证明: 当 n 为奇数时, 设 $n = 2k + 1$, 则 $2^{2k+1} - 1 = 2 \cdot 2^{2k} - 1 = 2 \cdot 4^k - 1 = 2 \cdot 4^k - 2 + 1 = 6 \left[\frac{1}{3} (4^k - 1) \right] + 1$ 。易知 $3 \mid 4^k - 1$, 为非负整数。

此时取 $m = \frac{1}{3}(4^k - 1)$, 显然有 $2^n - 1 = 6m + 1$, 同

理可知当 n 为偶数时 $2^n - 1 = 6m + 3$ 。

当 $v = 2^n - 1$ 中 n 为偶数时, $\text{NTS}(v)$ 为一RBIB, 即一科克曼三连系, 于是有:

系理. $\text{NTS}(4^k - 1)$ 是一个 $4^k - 1$ 阶Kirkman三连系。取 $k = 2$, $\text{NTS}(15)$ 即成为科克曼女生问题的解, 当非偶然。

我们知道, 区组设计各元、各区组间是没有规定顺序的, $\text{NTS}(v)$ 也一样, 只是各元大小有别, 这一点不属于设计的范围。 $\text{NTS}(v)$ 只是一种特殊的STS (v) 。由陆家羲的大集定理表明, 对 $\text{NTS}(2^n - 1)$ 而言, 存在着与它不相交的、另外的 $2^n - 4$ 个 STS $(2^n - 1)$, 它们都不必具备Nim三连系的性质1, 2, 3, 4以及下面的性质6。

引理, 如果 $\gamma = [\log, c]$, $2^\gamma \in C = A \triangle B$, 在映射 φ 下, $a > b$ 的充要条件是 $2^\gamma \in A$ 。

证明: $2^\gamma \in A \implies 2^\gamma \notin B$, 否则, $2^\gamma \in A$ 且 $2^\gamma \in B \implies 2^\gamma \in A \cap B$, 但已知 $2^\gamma \in A \triangle B = (A \cup B) \setminus (A \cap B) \implies 2^\gamma \notin A \cap B$, 矛盾。在 φ 下,

(i) $2^\gamma \in A, 2^\gamma \notin B \implies 2^\gamma \in A \cap \bar{B}, 2^\gamma \notin B \cap \bar{A} \implies 2^\gamma \in \bar{B}, 2^\gamma \notin \bar{A}$, 又 $\gamma = [\log, c]$, 即 2^γ 是 $C = A \triangle B = \bar{B} \cap \bar{A}$ 中的最大元素 $\implies \bar{b} > \bar{a}$ 。因 $\bar{B} \cup (A \cap B) = (\bar{B} \cup A) \cap (\bar{B} \cup B) = A \cap (A \cup B) = A, \bar{A} \cup (A \cap B) = (\bar{A} \cup A) \cap (\bar{A} \cup B) = B$, 记 $A \cap B = F, F \longleftrightarrow f$, 故

$a = f + \bar{b} > \bar{a} + f = b$, 即 $a > b$ 。

(ii) 在映射 φ 下, $A = \bar{B} \cup (A \cap B) = \bar{B} \cup F, B = \bar{A} \cup (A \cap B) = \bar{A} \cup F$. $a = \bar{b} + f, b = \bar{a} + f, a > b \implies \bar{b} > \bar{a}$. 已知 $2^r \in C = A \Delta B \implies 2^r \in (A \cap \bar{B}) \cup (B \cap \bar{A}) \xRightarrow{*} 2^r \in \bar{B} \cup \bar{A}$. $2^r \in \bar{B}$ 且 $2^r \in \bar{A} \implies 2^r \in \bar{B} \cap \bar{A} = \phi$, 此不可能。故知 $2^r \in \bar{B}$ 或 $2^r \in \bar{A}$ 。因 $r = \lfloor \log_2 c \rfloor$, 2^r 是 \bar{A} 或 \bar{B} 中最大元。假设 $2^r \in \bar{A}$, $2^r \notin \bar{B} \implies \bar{a} > \bar{b}$ 与已知矛盾。故知 $2^r \in \bar{B}$, $2^r \notin \bar{A} \implies 2^r \in A \cap \bar{B} \implies 2^r \in A$ 。证完。

由这个引理可以得到:

性质 6. 如果 $\{a', b, c\}, \{a, b', c\}, \{a, b, c'\}$ 是 Nim 三元组, 那么 $a' > a, c' > c \implies b' < b$ 或 $a' > a, b' > b \implies c' < c$ 。

证明: 在映射 φ 下, $A' = B \Delta C, B' = A \Delta C, C' = A \Delta B$ 。设 $A \Delta B \Delta C = D, 2^\delta \in D, \delta = \lfloor \log_2 d \rfloor$ 。由引理知

$$\begin{aligned} a' > a &\implies 2^\delta \in A' = B \Delta C, 2^\delta \notin A \\ c' > c &\implies 2^\delta \in C' = A \Delta B, 2^\delta \notin C \\ &\implies 2^\delta \in B, \end{aligned}$$

$2^\delta \notin B' = A \Delta C \implies b > b'$ 。同理 $a' > a, b' > b \implies c' < c$ 。证完。

性质 6 对 a' 所作的结论, 对 b' 或 c' 也成立。它的意义是: 当从 Nim 三元组 $\{a', b, c\}$

的一元 a' 中减去一个正整数 $x_1 (1 \leq x_1 < a')$ ①, $a' - x_1 = a$, 因 $A \triangle B \triangle C = D \neq \phi$, 所得 $\{a, b, c\}$ 非 Nim 三元组; 但在 b, c 之中, 恰有一个减去唯一确定的正整数 $x_2 (1 \leq x_2 < b \text{ 或 } 1 \leq x_2 < c)$: $b - x_2 = b'$, 或 $c - x_2 = c'$, 所得 b' 或 c' 使 $\{a, b', c\}$ 或 $\{a, b, c'\}$ 仍是一个 Nim 三元组。简言之, Nim 三连系对这两次减法“封闭”。

在 Nim 游戏中, 规则要求“至少取一个, 至多取一堆”, 即是 $1 \leq x_1 \leq a'$, $1 \leq x_2 \leq b$ 或 $1 \leq x_2 \leq c$ 。当取一堆时, 三元组变为二元组。由此可见, 抓三堆 Nim 的实质是: Nim 三元组三个元分解成的 2 的幂集中, 相等的元素恰能保持一一对应, 处于平衡状态; 减去 x_1 破坏了这种对应和平衡; 但又恰好存在 x_2 , 在作第二次减法后又恢复了这种对应和平衡。所以, 如果双方均掌握了制胜规律, 谁处在要破坏平衡的位置谁负, 谁处在恢复平衡的位置谁胜。

关于 Nim 的问题, 当然也可不用集合论的知识, 通过别的途径而解决。这里, 只是想说明, 有些貌似无关的知识之间, 可以建立联系; 而且, 人们在生产活动之外, 例如文化娱乐活动中, 也可以找到数学产生的源泉。组合数学最早起源于游戏, 这一点丝毫不能说明它就没有理论上和应用上的价值。也许, 起源于游戏的数学问

① 若 $x_1 = a'$ 或 $a = b$ 或 $a = c$ 结果都是平凡的。这里考虑 $x_1 \neq a'$, $a \neq b$, $a \neq c$ 的情况。

题，它的价值在人类生产活动中得到体现之后，才能得到本质上的发展；也许，当文化娱乐活动在人类总活动中所占比重愈来愈大时，这些活动也成为人类实践的一部分。人们乐意在娱乐中寻找他感兴趣的科学——于是，数学便按它自身的规律发展，把一些唠唠叨叨置之脑后了。

附录

平衡不完全区组与可分解
平衡不完全区组的构造方法

陆 家 羲

(一九六五年三月十四日)

(一) 引 言

§1. 给定一含有 v 个元素的集 τ , 叫做大小为 k 的区组是由 τ 中取 k 个元素的一个排列, 其中同一元素允许重复。具有一定性质的区组集叫做区组设计。区组常以 b 来代表, 区组集常以 S 来代表。元素 ξ 在 b 中出现的次数叫做 ξ 在 b 中的重复数; 对 S 中的各个区组计算重复数, 最后把它们加起来, 得到的数字叫做 ξ 在 S 中的重复数。若 b 中第 α 个元素是 ξ , 第 β 个元素是 ξ' , 我们说 ξ 和 ξ' 在 b 中以序 (α, β) 相遇。具有这种性质的不同数偶 (α, β) 的个数叫做 ξ 和 ξ' 在 b 中的相遇数; 对 S 中的各个区组计算相遇数, 最后把它们加起来, 得到的数字叫做

ξ 和 ξ' 在 S 中的相遇数, 用 $A_S(\xi, \xi')$ 来表示。显然 $A_S(\xi, \xi') = A_S(\xi', \xi)$ 。若 τ' 和 $\tau'' \subset \tau$, 定义 $A_S(\tau', \tau'') = \sum_{\substack{\xi \in \tau' \\ \xi' \in \tau''}} A_S(\xi, \xi')$ 。

具有下面这些性质的设计 S 叫做平衡不完全区组:

- (i) 每个区组的大小等于给定的常数 k ;
- (ii) $A_S(\xi, \xi) = 0$, 即任一区组无重复元素;
- (iii) 对任意的 ξ 和 $\xi' \in \tau (\xi \neq \xi')$, $A_S(\xi, \xi')$ 等于给定的常数 λ 。

平衡不完全区组以详略的不同, 用记号 $B[k, \lambda, v]$ 或 B 来表示。经简单的考察可以证明, τ 中任意元素在 B 中的重复数等于一定的常数, 并且它的参数满足下面的条件:

$$\left. \begin{aligned} \lambda(v-1) &\equiv 0 \pmod{(k-1)}, \\ \lambda v(v-1) &\equiv 0 \pmod{k(k-1)}, \end{aligned} \right\} \quad (1)$$

如果 v 是 k 的倍数, 即

$$v \equiv 0 \pmod{k}, \quad (2)$$

若能把 B 的全体区组分成各个行 (行常以 h 来代表), 使得每一元素在每一行中恰好出现一次, 这种设计叫做可分解平衡不完全区组, 用记号 $RB[k, \lambda, v]$ 或 RB 来表示。

条件 (1) 和条件 (1) (2) 对于构造 B

和 RB 是必要的, 但不一定充分①。本文给出 B 和 RB 的几种构造方法, 作为应用这些方法的例子, 证明了对构造 $\lambda=1, k=3$ 和 4 的 RB , 条件 (1) 和 (2) 是充分的。

§2. 设计 $B[k, \lambda, v]$ 可能由设计 $B[k, \lambda, v']$ 添加其他的区组而得到, 为表明这种性质, 这样得到的设计记为 $B_{v'}[k, \lambda, v]$ 。同样, 由 $RB[k, \lambda, v']$ 添加其他的区组而得到的 RB 就记为 $RB_{v'}[k, \lambda, v]$; $RB[k, \lambda, v']$ 的同一行的任意两个区组仍在 $RB_{v'}[k, \lambda, v]$ 的同一行中。

$B[k, \lambda, v]$, $B_{v'}[k, \lambda, v]$, $RB[k, \lambda, v]$ 和 $RB_{v'}[k, \lambda, v]$ 可以构造的事实分别用 $v \in B(k, \lambda)$, $v \in B_{v'}(k, \lambda)$, $v \in RB(k, \lambda)$ 和 $v \in RB_{v'}(k, \lambda)$ 来表示。当元素数为 0 或 1 时根本没有相遇的问题, 因此可以规定, 对任意的 k 和 λ , $0 \in RB(k, \lambda)$, $1 \in RB(k, \lambda)$ 。

$RB[k, \lambda, 0]$ 和 $RB[k, \lambda, 1]$ 的区组数均为 0。由以上定义显然有:

$$v \in RB(k, \lambda) \implies v \in B(k, \lambda),$$

$$v \in RB_{v'}(k, \lambda) \implies v \in B_{v'}(k, \lambda),$$

$$v \in RB_{v'}(k, \lambda) \implies v' \in RB(k, \lambda),$$

① 对于 $k=3, 4$ (和所有的 λ) 以及 $k=5, \lambda=1, 4, 20$, 条件 (1) 是充分的, 但 $B[5, 1, 141]$ 是可能的例外

$$v \in B_{v'}(k, \lambda) \implies v' \in B(k, \lambda).$$

而当 $v > 1$ 时,

$$\begin{aligned} v \in RB(k, \lambda) &\iff v \in RB_k(k, \lambda) \iff v \in \\ &RB_1(k, \lambda) \\ &\iff v \in RB_0(k, \lambda), v \in B(k, \lambda) \iff v \in \\ &B_K(k, \lambda) \\ &\iff v \in B_1(k, \lambda) \iff v \in B_0(k, \lambda). \end{aligned}$$

§ 3. 文中某些记号须先予说明。

1. 包括自 1 到 m 的正整数集我们用 $E(m)$ 来表示。一般的元素集用 τ 或 σ 来表示。欲说明集中元素的个数为 m , 使用记号 $\tau(m), \sigma(m)$ 。

2. 本文只对互不相交的集合考虑其和, 因此, $\tau = \tau' \cup \tau''$ 表示 τ 是互不相交的 τ' 与 τ'' 的和集。 $S = S' \cup S''$ 表示 S 是由合取 S' 和 S'' 的全体区组所构成。 $\xi \in S, S' \subset S$, 分别表示 ξ 是 S 中所含的元素, S' 是 S 的部分区组集。

3. $\tau = \sigma\sigma'$ 表示 τ 是 σ 和 σ' 的直积, 即 $\tau = \{(x, y); x \in \sigma, y \in \sigma'\}$, 而 $(x, y) = (x', y') \iff x = x'$ 和 $y = y'$ 。 x 叫做 (x, y) 在 σ 上的投影, y 叫做 (x, y) 在 σ' 上的投影, 分别用 $P_{\sigma}((x, y))$ 和 $P_{\sigma'}((x, y))$ 来表示。 逆投影 $P_{\sigma'}^{\sigma}(x)$ 和 $P_{\sigma}^{\sigma'}(y)$ 分别表示 σ 上投影是 x 和 σ' 上投影是 y 的 τ 中的元素集。 以上定

义和记号可以推广至多个集的积。例如 $P_{\sigma\sigma'\sigma''}^{\sigma\sigma'\sigma''}(\xi)$ 和 $P_{\sigma\sigma'\sigma''}^{\sigma\sigma'\sigma''}(\xi)$ 分别表示 $\sigma\sigma'\sigma''$ 中元素 ξ 在 σ 和 σ' 上的投影。

(二) (S, T) 和 (S, RT)

§4. 由 $\sigma(m)$ 的元素构成的具有以下性质的设计记以 $T[k, m]$ (简称 T):

(i) 每个区组的大小为 k ;

(ii) 任意给定 x 和 $x' \in \sigma$, α 和 $\beta \in E(k)$ ($\alpha \neq \beta$), $T[k, m]$ 内恰好有一个组 b , 使 x 和 x' 在 b 内以序 (α, β) 相遇。

如果 $T[k, m]$ 的全体区组被分成各个行, 使得对任一元素 $x(x \in \sigma)$ 和任一整数 $a(a \in E(k))$, 每行恰有一组它的第 a 个元素是 x , 这种设计我们记为 $RT[k, m]$ (简称 RT)。 $T[k, m]$ 和 $RT[k, m]$ 可以构造的事实分别用 $m \in T(k)$ 和 $m \in RT(k)$ 来表示。

§5. 【命题1】 $m \in T(k) \iff m \in RT(k-1)$ ($k \geq 3$)。

证明: 于 $RT[k-1, m]$ 的同一行的各个区组的末尾加入同一个元素, 可以构成 $T[k, m]$ 。相反, 使 $T[k, m]$ 的末一个元素相同的区组排在同一行, 去掉这个元素后就得到 $RT[k-1, m]$ 。

【命题2】

(i) 若 $m = \prod_{i \in E(S)} p_i^{a_i}$ (p_i 是素数, a_i 是正整

数), 且对任意的 $i \in E(S)$, $p_i^{a_i} \geq k$ (k 是正整数), 则 $m \in T(k+1)$, $m \in RT(k)$;

(ii) 若 $m \neq 2$, $m \neq 6$, 则 $m \in T(4)$, $m \in RT(3)$ 。

证明: 构造 $T[k, m]$ 等价于构造正交阵列表 $OA(m^2, k, m, 2)$ 或 $k-2$ 个互相正交的拉丁方, 由正交拉丁方的已知结果即得此命题【2】【3】【4】。

§6. 设给定一大小为 k 的区组 b 和设计 $T[k, m]$ 。取 $T[k, m]$ 中的一个区组 b' 。若 b 中第 α 个元素是 x , b' 中第 α 个元素是 y , 我们写出一新的元素 (x, y) 。对所有的 $\alpha (\alpha \in E(k))$ 写出来的 k 个元素按原来的次序排列使之组成一个区组。令 b' 遍历 $T[k, m]$ 的全体区组而完成以上手续, 所得的区组集记为 (b, T) 。若所给定的是一个 $RT[k, m]$, 并把根据 RT 中同一行的组所构成的区组组成一行, 这样得到的设计我们记为 (b, RT) 。

如果 S 的每个区组的大小是 k , 定义 $(S, T) = \bigcup_{b \subset S} (b, T)$, $(S, RT) = \bigcup_{b \subset S} (b, RT)$ ($(b, R$

$T)$ 的每一行仍是 (S, RT) 的行 ($b \subset S$)。

§ 7. 【命题】设 S 中的元素属于 σ , $T[k, m]$ 和 R $T[k, m]$ 中的元素属于 σ' , 可知:

- (i) (S, T) 中的元素属于 $\sigma\sigma'$;
- (ii) 任意给定元素 ξ 和 $\xi' \in \sigma\sigma'$, 则 $A_{(S, T)}(\xi, \xi') = A_S(P_{\sigma\sigma'}^{\sigma}(\xi), P_{\sigma\sigma'}^{\sigma'}(\xi'))$;
- (iii) 若 $x \in b^{\sigma}$, $b \subset S$, 则 $P_{\sigma\sigma'}^{\sigma}(x)$ 中的每一元素在 (b, RT) 的每一行中的重复数等于 x 在 b 中的重复数。

证明: 1. (i) 据定义显然。

2. 设 ξ 和 $\xi' \in \sigma\sigma'$, 它们在 (b, T) 的某个组 b'' 以序 (α, β) 相遇 ($b \subset S$)。据定义知 $P_{\sigma\sigma'}^{\sigma}(\xi)$ 和 $P_{\sigma\sigma'}^{\sigma'}(\xi')$ 在 b 中亦以序 (α, β) 相遇。相反, 若 $P_{\sigma\sigma'}^{\sigma}(\xi)$ 和 $P_{\sigma\sigma'}^{\sigma'}(\xi')$ 在 b 中以序 (α, β) 相遇, 那么在 $T[k, m]$ 中恰有一个区组 b' , 使 ξ 和 ξ' 在从以作得的 (b, T) 的区组 b'' 中以序 (α, β) 相遇。由此见 (ii) 成立。

3. 设 $b \subset S$, $\xi \in \sigma\sigma'$, x 是 b 的第 α 个元素, 当 $\xi \in P_{\sigma\sigma'}^{\sigma}(x)$, ξ 不可能以序 α 出现在 (b, RT) 的某一组中; 而当 $\xi \in P_{\sigma\sigma'}^{\sigma'}(x)$, 则 ξ 在 (b, RT) 的某组 b'' 以序 α 出现的条件是, $P_{\sigma\sigma'}^{\sigma'}(\xi)$ 以序 α 出现在 b'' 据以作成的组 b' 中 ($b' \subset RT$)。但在 RT 的每一行内适合这个条件的 b' 恰有一个, 由此见 (iii) 成立。

(三) 构造 B 的差集合方法①

(四) 构造 RB 的差集合方法②

(五) 构造 RB 的组合方法②

(六) $k=3, \lambda=1$ 的 RB ②

(七) $k=4, \lambda=1$ 的 RB

§25. 记正整数集 C_2 , 其中每一个整数 R 存在下面的素数幂分解式:

$$R = \prod_{i \in E(S)} p_i^{\alpha_i}, \quad p_i^{\alpha_i} = 1 + 4t_i (i \in E(S), t_i \text{ 是}$$

正整数) (8)

【命题】若 $R \in C_2$, 则 $(3, R) \in FE(4, 1, 1)$.

证明: 依 §10 从分解式 (8) 确定环 K .
令 $H_j = \{e_j, -e_j, \eta_j, -\eta_j\}$, 这里 η_j 在 $GF_i(P_i^{\alpha_i})$ 上的投影若不是据 G_j 的定义为 0 即等于 g_i^{-1} (g_i 是 $GF_i(P_i^{\alpha_i})$ 的元根)。显然有 $\eta_j^2 = -e_j$. 命 $\tau = MK$, M 是阶为 3 的剩余模, 则下面的区组 b 使构成 $FE[4, 1, 1, 3, R]$ 中的 FS_j :

$$b = [(1, e_j)(1, -e_j)(2, \eta_j)(2, -\eta_j)].$$

§26. 【命题】若 $R \in C_2$, 则 $1 + 3R \in RB(4, 1)$.

证明: 据 §15, 只须证明 $R \in RFY_1(4, 1, 3)$. 命 $\tau = \{a\} \cup MK$, M 和 K 的意义同 §25.

① 见本书第七节。

② 见本书第九节。

据 §13 及 §25 可以构造 $FY_1[4, 1, 3, R]$, 由下面的区组集所构成:

$$[a, (0, 0)(1, 0)(2, 0)] \cup \Phi_M$$

$$\left(\bigcup_{j \in E(2^s - 1)} \right) \langle FS_j, A_j \rangle$$

最后只须验明此区组集满足 §15 的甲种行的条件。

§27. 【命题】若 $R \in C_s$, 则 $R \in RFY_1(4, 1, 12)$ 。

证明: 依 §25 中的方法确定 K 和 M 并构造 $FE[4, 1, 1, 3, R]$ 。取阶为 4 的剩余模 M' 的元素构造 $RT[4, 4]$, 从而构造 (FE, RT) 。由 §11 可知它是 $M'MK$ 中元素组成的 $FE'[4, 1, 4, 3, R]$, 并且 FE' 的每个 ES_j' 由 4 个行 $h^x_j (x \in M')$ 所组成 (见 §6) 。①

取集合 $\tau'(4) \cup M'MG_{s,1}$, 以之构造 $RB_s[4, 1, 16]$ (§26), 包含 τ' 的全体元素组成的

区组 b' 。然后构造 $\Phi_M \left(\bigcup_{j \in E(2^s - 1)} \langle FS_j', A_j \rangle \right)$

$\cup RB_s$, 在取去其中的组 b' 后, 由 §13 知所得是 $FY_1[4, 1, 12, R]$, 其元素属于 $\tau = \tau' \cup M'$

①实际上, 据 §11 $FS_j' = (b, RT)$, b 的意义见 §25。——陆家羲注。

MK 。令 RB_i 中被取去组 b' 的行所剩下的部分组成一新的行，它满足 §15 的乙种行的条件， FY_i 的其余区组可以组成 4 个甲种行 $h_x (x \in M')$ ：

$$h_x = \Phi_M \left(\bigcup_{j \in E(2^s - 1)} \langle h_j^x, A_j \rangle \right) \cup \tilde{h}$$

这里 \tilde{h} 是 RB_i 中不包含组 b' 的某一行。注意到 §7 (iii) 这一点便易于验明。 FY_i 的区组既然可以分成甲、乙种行，可见命题成立。

§28. 【命题】若 $R \in C_2$ ，则 $R \in RFY_{16}$ (4, 1, 12)。

证明：取按 §27 中方法构成的 RFY_{16} [4, 1, 12, R]，其元素属于 $\eta'(4) \cup M'MK$ 。命 $\sigma = \{\hat{1}, \hat{2}, \hat{3}, \hat{4}\}$ 。在集合 $\bigcup_{j \in E(2^s - 1)} A_j$ 中任取一元素

a ，假设 $a \in A_j$ 。然后从 RFY_i 的每一行 h_x 中取去区组集 $S_x (x \in M')$ ：

$$S_x = \Phi_M (\langle h_{j_0}^x, a \rangle),$$

代之以由 $\sigma M \cup M'MK$ 中元素构成的 S_x' ， $S_x' =$

$\bigcup_{y \in M} S_y^x$ ， S_y^x 如下面所示（属于 $MM'K$ 的元素

只写出其在 $M'M$ 上的投影，在 K 上的投影：

组中第一个元素为 a ，第二个元素为 $-a$ ，第三

个元素为 $a\eta_{j_0}$, 第四个元素为 $-a\eta_{j_0}$:

$$\begin{aligned}
 S_y^0: & [(3, y)(3, y)(3, 1+y)(3, 1+y)], \\
 & [(2, 2+y)(\hat{3}, y)(0, y)(1, y)], \\
 & [(\hat{2}, y)(1, 1+y)(2, 2+y)(0, 2+y)], \\
 & [(0, y)(2, y)(1, 1+y)(\hat{4}, y)], \\
 & [(1, y)(0, y)(\hat{1}, y)(2, 1+y)]; \\
 S_y^1: & [(2, y)(2, y)(2, 1+y)(2, 1+y)], \\
 & [(\hat{4}, y)(0, 1+y)(1, 2+y)(3, 2+y)], \\
 & [(0, 1+y)(3, 1+y)(\hat{3}, y)(1, 2+y)], \\
 & [(1, 1+y)(\hat{1}, y)(3, 2+y)(0, 2+y)], \\
 & [(3, y)(1, y)(0, 1+y)(\hat{2}, y)], \\
 S_y^2: & [(0, y)(0, y)(0, 1+y)(0, 1+y)], \\
 & [(1, y)(3, y)(2, 1+y)(\hat{4}, y)], \\
 & [(3, 1+y)(\hat{1}, y)(1, 2+y)(2, 2+y)], \\
 & [(2, 1+y)(1, 1+y)(\hat{3}, y)(3, 2+y)], \\
 & [(\hat{2}, y)(2, 1+y)(3, 2+y)(1, 2+y)]; \\
 S_y^3: & [(1, y)(1, y)(1, 1+y)(1, 1+y)], \\
 & [(3, y)(2, y)(\hat{1}, y)(0, 1+y)], \\
 & [(2, y)(0, y)(3, 1+y)(\hat{2}, y)], \\
 & [(\hat{4}, y)(3, 1+y)(0, 2+y)(2, 2+y)], \\
 & [(0, 2+y)(\hat{3}, y)(2, y)(3, y)].
 \end{aligned}$$

取代后 h_x 变成 h_x' , 对于集 $\tau' \cup \sigma M \cup M' M$
 K , h_x 满足甲种行的条件。再补充 4 个乙种
 行 h_x'' ($x \in M'$), 就得到 $RFY'_{16}[4, 1, 12, R]$,

$$h_x'' = \Phi_M(b_x), \quad b_x = [(x, 1, a) \quad (1+x,$$

$$1, -a) \quad (3+x, 2, a\eta_{j_0}) \quad (2+x, 2, -a\eta_{j_0})].$$

为了证明这一点, 只须验明其满足 §9 中的条件①。

§29. 【引】 若 $R \in C$, $q = 12t$, $4t \leq R - 1$, $4 + q \in RB(4, 1)$, 则 $4 + q + 12R \in RB_{4+q}(4, 1)$ 。

证明: 证明与 §24 引类似。据 §15 中的定理, 只须证明 $R \in RFY_{4+q}(4, 1, 12)$ 。当 $t = 0$ 和 1 时这已在 §27 和 §28 中证明, 但 §28 的 α 的选取可有 $\frac{R-1}{4}$ 种, 选取其中的 t 个进行分析

可得 $RFY_{4+q}[4, 1, 12, R]$ 。

【定理】 $v \in RB(4, 1)$ 的充要条件是 $v \equiv 4 \pmod{12}$ 。

证明: 必要性由 (1) 和 (2) 即得。设 $v = 4 + 12R'$ 。

1. $R' \geq 37$ 的情形: 写出 C 中整数的序列: 37, 45, 53, 65, 81, 101, 125, 153, 185, 则恒

① 为便于检验我们指出, 若单看元素在 M' 上的投影, 同

时把集 σM 的所有元素认作是相同的, 那么 $\tilde{b} \cup_{x \in M'} b_x$

和 $S_{x_0}(x \in M')$ 构成 $RT[4, 5]$ 的 5 个行, 这里 \tilde{b} 的全体元素均属于 σM 。——陆家羲注。

存在正整数 n 和序列中的整数 R_1, R_2 , 使下面两个式子成立:

$$5R_1 \leq R' < 5R_2, 4R_2 \leq 5R_1.$$

因此据引可以归结为下面的情形 (令引中的 $R = 5R_1$).

2. $R' < 37$ 的情形: 除却 $v = 100$, 都可以在前文中直接找到构造公式 (参阅附表二) 以下给出 $RFY_0[4, 1, 4, 25]$ 的一种构造, 从之可以构造 $RB[4, 1, 100]$ (§ 15). 设 g 是 $GF(25)$ 中的一个元根, 满足 $g^8 - 1 = g^q, q \equiv 1 \pmod{2}$

(这样的元根是存在的)。选择元素 a , 使下面的集 A 中所含的 $GF(25)$ 的八个元素互不相等:

$$A = \{0, 1, g^8, g^{10}, a, g^2 + a, g^{10} + a, g^{18} + a\}.$$

关于 $GF(25)$ 的 A 的补集记作 A^c .

命 $\tau = E(4)GF(25)$, 则由 τ 中元素构成的 $RFY_0[4, 1, 4, 25]$ 包括着一个甲种行 b 和八个乙种行 $hz (z \in A)$:

$$b = \bigcup_{\substack{Y \in E(4) \\ Z \in A^c}} (b, \cup b', \cup h_z) \textcircled{1},$$

$$b, = [(y, 0)(y, g^{8'}) (y, g^{8'+8'}) (y, g^{10'+8'})],$$

$$b, ' = [(y, ag^{8'}) (y, (g^2 + a)g^{8'}) (y, (g^{10} + a)g^{8'}) (y, (g^{18} + a)g^{8'})],$$

$$b, = [(4, z)(1, zg^8)(2, zg^{12})(3, zg^{18})].$$

〔附表一〕②③

〔附表二〕②③

〔文 献〕

- 【1】 H. Hanani, The existence and construction of balanced incomplete block designs, *Ann. Math. Stat.*, 32(1961), 361—386.
- 【2】 增山元三郎著、刘璋温译：《试验设计法》，上海科学技术出版社，1963年，66—71。
- 【3】 刘璋温：《尤拉方阵》，数学通报，1961年，9。
- 【4】 R.C. Bose, S.S. Shrikhande and E.T. Parker, Further results on the construction of mutually orthogonal latin squares and the falsity of Euler's conjecture, *Canad. J. Math* 12(1960), 189—203.
- 【5】 H.B. Mann著、张里千、刘璋温等译：《试验的分析与设计》，科学出版社，1964年，97—99。
- 【6】 增山元三郎著、刘璋温译：《试验设计法》，上海科学技术出版社，1963年，52—57。
- 【7】 W.W.R. Ball, *Mathematical Recreations and Essays*, Macmillan, London, 1956, Chapter X.
- 【8】 F.N. Cole, Kirkman parades, *Bull. Amer. Math. Soc.*, 1922, 435—437.
- 【9】 M. Hall, Jr, A survey of Combinatorial Analysis, *Some Aspects of Analysis and*

Probability, John. Wiley & Sons, New York, 1958, 76—104.

【10】 Claude Berge 著、李修睦译：《图的理论及其应用》，上海科学技术出版社，1963, 258。

【11】 A. Caley: Phil. Magaz. 37(1850), 52.

【12】 E. Netto: Lehrhuch der Combinatorik, Teubner, Leipzig, 1927, §145.

① 实际上, $b_1 U b_1'$ 是 $FY_0[4, 1, 1, 25]$, $\Phi_{GF}(b_1 U b_1')$ 是 $B[4, 1, 25]$. 参阅文献[6]表11.1中的 F_1 系统。——陆家羲注。

② 以至少给出一种构造方法为原则。——陆家羲注。

③ 原文缺此二表。——本书作者注。

参 考 文 献

- 〔1〕孙泽瀛,《数学方法趣引》, 中国科学图书仪器公司(1953)93.
- 〔2〕Berge C., The Theory of Graphs and Its Applications, Methuen (1962).
- 〔3〕Fraenkel A.S., Never rush to be first in playing Nimbi, Mathematics Magazine, 53,1 (1980) 22.
- 〔4〕Brualdi R.A., Introductory Combinatorics, (1977) by Elsevier North-Holland, Inc., 中译本见李盘林、王天明译《组合学导引》, 华中工学院出版社(1982).1.
- 〔5〕The Oxford English Dictionary, Vol.VII, 151.
- 〔6〕Webster's Third New International Dictionary, (1937) 1528.
- 〔7〕谈祥柏,《趣味对策论》, 中国青年出版社(1982), 45.
- 〔8〕徐利治: 组合数学——现代组合分析学, 《自然杂志》, No. 10., (1980), 751.
- 〔9〕柯召、魏万迪,《组合论》上册, 科学出版社(1981)前言.
- 〔10〕罗见今, 世界上最古老的三阶幻方——关于组合学起源的讨论, 《自然辩证法通讯》3(1986)

49—57.

- [11] Ryser H. J., *Combinatorial Mathematics*,
Published by the Math. Assoc. of Amer-
ica, (1963) 1. 中译本见李乔译《组合数学》,
科学出版社(1983)1,.
- [12] Доморяд А. И., *Математические игры
и развлечения*, 中译本见杨之译《数学博弈与
游戏》, 科普出版社(1985), 72.
- [13] Brylawski T., *Combinatorial Theory*, E-
ncyclopedia of Science & Technology, Mc
Graw-Hill Book Co. 4th ed (1977). 中译本
见《科学技术百科全书》第1卷数学, 356.
- [14] Euler L., *Recherches sur une nouvelle e-
specie de carre's magiques* Verh. Zeeu-
wsch. Genootsch. Wetensch Vlissingen
9, (1781) 85—239.
- [15] Bose R. C., Parker E. T., Shrikhande S.
S., Further results on the constrction
of mutually orthogonal Latin squares
and the falsity of Euler's conjection,
Canadian Journal of Mathematics 12
(1960), 189—203.
- [16] Dictionary of Scientific Biography, Vol.
VII (1973), U. S. A. 383—384.
- [17] Combrige and Dublin Math. J.
- [18] London, Edinbergh and Dublin Philos.
Mag. and J. Sci.
- [19] Kirkman T. P., Query VI.. Lady's and

- Gentleman's Diary, (1850), 48.
- [20] Kirkman T.P., Solution to Query VI.,
Lady's and Gentleman's Diary, (1851), 48.
- [21] 康庆德, 斯坦纳和科克曼三元系及大集问题,
《自然杂志》8卷6期(1985), 459.
- [22] Denniston R.H.F., Some packings with
Steiner triple systems, Discrete Math.
9(1974), 213—227.
- [23] Kirkman T.P., On the puzzle of the fif-
teen young ladies, Combridge and Dublin
Math. J., (4) 23(1862), 198—204.
- [24] Biggs N.L., T.P. Kirkman, mathematician,
Bull. London Math. Soc. 13(1981), 97
—120.
- [25] See [16], Vol. XIII, 216—222.
- [26] Bliss G.A., The scientific Work of Elia-
kim Hastings Moore, Bulletin of the
Amer. Math. Soc. 40(1934), 501—514.
- [27] Horton J.D., Variations on a theme by
Moore, Proc. Louisiana conf. Combinato-
rics, Graph Theory and Computing (1970)
146—166.
- [28] Ball W.W.R., Mathematical recreations
and problems, 1st ed. London (1892).
Math. recreations and essays, 11th ed.
Mac Millan. London (1939).
- [29] Cayley A., On the triadic arrangements
of seven and fifteen things, see [18], (3)

- 37(1850), 50—53 (Collected Math. Papers I, 481—484).
- [30] 见 [9], 159.
- [31] Kirkman T.P., On a problem in combinations, see [17], 2(1847), 191—204.
- [32] Sylvester J.J., Elementary researches in the analysis of combinatorial aggregation, see [18], (3) 24(1844), 285 —296 (Collected Math. Papers, I, 91—102).
- [33] Woolhouse W.S.B., Prize question 1733, Lady's and Gentleman's Diary (1844).
- [34] See [16], Vol. III, 162—170.
- [35] Spottiswoode W., On a problem in combinatorial analysis, see [18], (4) 3 (1852), 348—354.
- [36] Ansttice R.R., On a problem in combinations, see [17], 4(1852), 279—292 and 8(1853), 149—154.
- [37] Steiner J., Combinatorische Aufgabe, J. rein angew. Math. 45(1853), 181—182 (Gesammelte Werke, II 435—438).
- [38] See [16], Vol. XIII, 12—22.
- [39] Clausen T., Über eine combinatorische Aufgabe, Archiv Math. Phys. (1) 21 (1853), 93—96.
- [40] Reiss M., Über eine Steinersche combinatorische Aufgabe, welche in 45 sten Bände dieses Journals seit 181, gestellt

- wordenist, J. reine angew. Math. 56(1859), 326—344.
- [41] Hanani H., The existence and construction of balanced in complete block designs, Ann. Math. Statist. 32 (1961). 361—386.
- [42] Wilson R. M., An existence theory for pair-wise balanced designs, J. Combinat. Theory (A) 18(1975), 71-79.
- [43] Bose R.C., On the construction of balanced incomplete block designs, Ann. Eugenics, 9(1939). 353—399.
- [44] Moore, E.H., Concerning triple systems, Math. Ann. 43 (1893), 271—285.
- [45] Hall, M.Jr., Combinatorial Theory, Waltham, Mass. (1967).
- [46] 陆家羲手稿, 1983, 5, 30. 现存内蒙师大数学系。
- [47] Ray-Chaudhuri D.K., Wilson R.M., Solution of Kirkman's schoolgirl problem, Proc. Symp. Pure Math. 19(1971). Amer. Math. Soc., Providence, R.I., 187—203.
- [48] Ray-chaudhuri D.K., Wilson R.M., The existence of resolvable block designs, A survey of Combinatorial Theory, North Holland, Amsterdam (1973), Chap. 30, 361—375.
- [49] 陆家羲, 《可分解平衡不完全区组设计的存在

- 性理论》，数学学报，27卷4（1984）。
- [50] 吴利生，《关于 $S(2,3,V)$ 的大集和 RBIB 的存在性问题》，数学研究与评论1（1984），151—154.
- [51] Bays S., Use question de Cayley relative au problème des triades Steiner, Enseignement Math. 19(1917), 57—67.
- [52] Kramar E.S., Mesner D.M., Intersections among Steiner Systems, J. Combinat. Theory (A) 16 (1974), 273—285.
- [53] Kramar E.S., Mesner D.M., The possible(impossible) systems of 11 disjoint $S(2,3,13)$'s ($S(3,4,14)$'s) with automorphism of order 11, Utilitas Math, 7 (1975), 55—58.
- [54] Rosa A., Intersection properties of Steiner systems, Annals of Discrete Math. 7 (1980), 115—128. in: Topics on Steiner System (Ed. C.C. Lindner and A. Rosa).
- [55] Sylvester J. J., Remark on the tactic of nine elements, see [18], (4) 22 (1861), 144—147 (Collected Math. Papers, II. 288—289).
- [56] Sylvester J. J., Note on a nine school-girls problem, Messenger Math. (2) 22 (1892—93), 159—160. Correction: 192. (Collected Math. Papers, IV, 732—733).
- [57] See Lucas E., Récréations mathématiques

- Vol. 2, Gauthier-Villaris, Paris 1883
(Sixième récréation: Lesjeux de demoiselles, 161—197).
- [58] Emch A., Triple and multiple system, their geometric configurations and groups, Trans. Amer. Math. Soc. 31 (1929), 25—42.
- [59] Assmus E.F.Jr., Mattson H. F.Jr., Steiner systems and perfect codes, University of North Carolina Institute of Statistics Mimeo Series No. 481—1 (1966).
- [60] Assmus E.F.Jr., Mattson H.F.Jr., Research problem, J. Combinat. Theory 3 (1967), 307.
- [61] Doyen J., Construction of disjoint Steiner triple systems, Proc. Amer. Math. Soc. 32(1972) 409—416.
- [62] Teirlinck L., On the maximum number of disjoint Steiner triple systems, Discrete Math. 6(1973), 299—300.
- [63] Skolem Th., Some remarks on the triple Systems of Steiner, Math. Scand. 6(1958), 273—280.
- [64] Beenker G.F.M., Gerards A.M.H., Penning P., A construction of disjoint Steiner triple systems, TH Report 78—WSK—01, Dept. of Math. Technological Univ. Eindhoven.

-
- [65] Kotzig A., Lindner C.C., Rosa A., Latin squares with no subsquares of order two and disjoint steiner triple systems, *Utilitas Math.* 7(1975), 287—294.
- [66] Rosa A., A theorem on the maximum number of disjoint Steiner triple systems, *J. Combinat. Theory (A)* 18(1975), 305—312.
- [67] Teirlinck L., *Combinatorial Structures*, Thesis, Vrije Universiteit Brussel, Dept. voor Wiskunde (1976), 106pp.
- [68] Denniston R.H.F., Some packings with Steiner triple systems, *Discrete Math.* 9(1974), 213—227.
- [69] Denniston R.H.F., Sylvester's problem of the 15 schoolgirls, *Discrete Math.* 9(1974), 229—233.
- [70] Schreiber S., Covering all triples on n marks by disjoint Steiner systems, *J. Combinat. Theory (A)* 15(1973), 347—350.
- [71] Wilson R.M., Some partitions of all triples into Steiner triple systems. *Hypergraph Seminar* (Ohio State Univ. 1972), *Lecture Notes Math.* 411 (Springer, Berlin 1974) 267—277.
- [72] Lindner C.C., On the number of disjoint Mendelsohn triple systems, *J. Combinat. Theory (A)* 30(1981), 326—330.

-
- [73] Lu Jia—Xi, On Large sets of disjoint Steiner triple systems I, I, II, J. Combinat. Theory (A), 34(1983), 140—182.
- [74] Lu Jia—Xi, On large sets of disjoint Steiner triple systems, N, V, N, J. Combinat. Theory (A), 37(1984), 136—192.
- [75] 康庆德, 《LD 设计的一个递归构造》, 应用数学学报4(1987), 481—490.
- [76] 1987年国家自然科学奖获奖项目, 《科技日报》1988年3月18日, 第2版。
- [77] 包头市编: 《向陆家羲同志学习》, 1984年5月, 共48页。
- [78] 高桥磐郎, 组合せ理論とその 应用, 岩波全书316(1979)序论。
- [79] Fisher R.A., Yates F., Statistical table's for biological, agricultural and medical research, Oliver and Boyd, Edinburgh(1938).
- [80] Doehlert D.H., Balanced sets of balanced incomplete block designs of block size three, Technometrics 7(1965), 561—577.
- [81] Doyen J., Rosa A., A bibliography and survey of Steiner systems (1983) (to appear). pp. 115.
- [82] Eckenstein O., Bibliography of Kirkman's school-girl problem, Messenger Math. (2) 41(1911—12), 33—36.
- [83] Ahrens W., Mathematische Unterhaltungen und Spiele, Vol. 2, Leipzig. (1918).

-
- [84] Doyen J., Recent results on Steiner triple systems, *Finite Geometric Structures and their Applications* (C.I.M.E. II Ciclo Bressanone 1972), Edizioni Cremonese, Roma 1973, 201—210.
- [85] 罗见今, Steiner 系若干课题研究的历史回顾, *数学进展*, 15卷2期(1986), 175—184.
- [86] Doyen J., Rosa A., A bibliography and survey of Steiner Systems, *Bolletino della Unione Matematica Italiana* (4)7(1973), 392—419.
- [87] Кирилов, А.А., Теоремы и задачи функционального анализа, Москва (1979). стр. 19.
- [88] 沈石山, 《集合论初步》(1980), 47.

译 名 对 照

(按译名拼音字母顺序)

安斯梯斯	R. R. Anstice
阿斯穆斯	E. F. Assmus
保尔	W. W. R. Ball
贝尔热	C. Berge
柏克霍夫	G. Birkhoff
贝斯	S. Bays
比格斯	N. L. Biggs
玻斯	R. S. Bose
布顿	C. L. Bouton
布鲁尔迪	R. A. Brualdi
布鲁劳斯基	T. Brylawski
戴维德和巴顿	Daivid and Barton
德尼斯顿	R. H. F. Denniston
棣莫甘	De Morgan
多耶勒特	D. H. Doehlert
多延	J. Doyen
费尔普斯	K. T. Phelps
费希尔	R. A. Fisher
哈密尔顿	Hamilton
哈纳尼	H. Hanani
哈特曼	A. Hatman
霍尔	M. Jr. Hall

加德纳	M. Gardner
凯莱	A. Cayley
考克斯特	H. S. M. Coxeter
科尔本	C. J. Colbourn
科克曼	T. P. Kirkman
克劳森	T. Clausen
克雷默	E. S. Kramer
莱布尼兹	Leibniz
莱塞	H. J. Ryser
雷·乔德赫里	D. K. Ray Chaudhuri
林德奈	C. C. Lindner
黎斯	M. Reiss
罗沙	A. Rosa
E. 曼德尔逊	E. Mendelsohn
N. 曼德尔逊	N. S. Mendelsohn
梅斯纳	D. M. Mesner
米尔斯	W. H. Mills
穆尔	E. H. Moore
穆林	R. C. Mullin
皮特·海因	Piet Hein
斯波梯斯乌德	W. Spottiswood
斯科勒姆	Th. Skolem
斯坦顿	R. G. Stanton
斯坦纳	J. Steiner
特林克	L. Teilinck
瓦勒斯基	Waleski
威尔逊	R. M. Wilson
伍尔豪斯	W. S. B. Woolhouse

西尔沃斯特

J.J.Sylvester

依姆希

A. Emch

伊萨克斯

R. Isaacs